

Privacy: An Overview of the Electronic Communications Privacy Act

Charles Doyle
Senior Specialist in American Public Law

March 30, 2011

GalleryWatch.com
http://www.crsdocuments.com
Penny Hill Press

Congressional Research Service
7-5700
www.crs.gov
R41733

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

This report provides an overview of federal law governing wiretapping and electronic eavesdropping under the Electronic Communications Privacy Act (ECPA). It also appends citations to state law in the area and the text of ECPA.

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given his prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than five years; fines up to $250,000 (up to $500,000 for organizations); in civil liability for damages, attorneys' fees and possibly punitive damages; in disciplinary action against any attorneys involved; and in suppression of any derivative evidence. Congress has created separate, but comparable, protective schemes for electronic communications (e.g., email) and against the surreptitious use of telephone call monitoring practices such as pen registers and trap and trace devices.

Each of these protective schemes comes with a procedural mechanism to afford limited law enforcement access to private communications and communications records under conditions consistent with the dictates of the Fourth Amendment. The government has been given narrowly confined authority to engage in electronic surveillance, conduct physical searches, and install and use pen registers and trap and trace devices for law enforcement purposes under ECPA and for purposes of foreign intelligence gathering under the Foreign Intelligence Surveillance Act.

This report is available in an abridged form without footnotes, quotations, attributions of authority, or appendixes as CRS Report R41734, *Privacy: An Abridged Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

Contents

Introduction 1
Background 1
Title III: Prohibitions 6
Illegal Wiretapping and Electronic Eavesdropping 6
Person 7
Intentional 7
Jurisdiction 7
Interception 8
Content 9
By Electronic, Mechanical, or Other Device 10
Wire, Oral, or Electronic Communications 11
Endeavoring to Intercept 12
Exemptions: Consent Interceptions 12
Exemptions: Publicly Accessible Radio Communications 14
Exemptions: Government Officials 14
Exemptions: Communication Service Providers 15
Domestic Exemptions 16
Illegal Disclosure of Information Obtained by Wiretapping or Electronic Eavesdropping 16
Illegal Use of Information Obtained by Unlawful Wiretapping or Electronic Eavesdropping 19
Shipping, Manufacturing, Distributing, Possessing or Advertising Wire, Oral, or Electronic Communication Interception Devices 20
Title III: Government Access 23
Law Enforcement Wiretapping and Electronic Eavesdropping 23
Title III: Consequences of a Violation 28
Criminal Penalties 28
Civil Liability 29
Civil Liability of the United States 30
Administrative Action 31
Attorney Discipline 31
Exclusion of Evidence 32
Stored Electronic Communications (SCA) 34
SCA: Prohibitions 34
SCA: Government Access 38
SCA: Consequences 42
Pen Registers and Trap and Trace Devices (PR/T&T) 44
PR/T&T: Prohibitions 44
PR/T&T: Government Access 45
PRT&T: Consequences 46

Appendixes

Appendix A. State Statutes Outlawing the Interception of Wire(w), Oral(o) and Electronic Communications(e) 48
Appendix B. Consent Interceptions Under State Law 49
Appendix C. Statutory Civil Liability for Interceptions Under State Law 50
Appendix D. Court Authorized Interception Under State Law 51
Appendix E. State Statutes Regulating Stored Electronic Communications (SE), Pen Registers (PR) and Trap and Trace Devices (T) 52
Appendix F. State Computer Crime Statutes 53
Appendix G. Spyware 54
Appendix H. Text of Electronic Communications Privacy Act (ECPA) 55

Contacts

Author Contact Information 84

GalleryWatch.com
http://www.crsdocuments.com

Introduction

Depending on one's perspective, wiretapping and electronic eavesdropping are either "dirty business," essential law enforcement tools, or both. This is a very general overview of the federal statutes that proscribe wiretapping and electronic eavesdropping and of the procedures they establish for law enforcement purposes. Although the specifics of state law are beyond the scope of this report, citations to related state statutory provisions have been appended. The text of pertinent federal statutes appears as an appendix as well.[1]

Background

At common law, "eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet; or are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behavior."[2] Although early American law proscribed common law eavesdropping, the crime was little prosecuted and by the late nineteenth century had "nearly faded from the legal horizon."[3] With the invention of the telegraph

[1] Portions of this report draw upon a series of earlier reports, no longer available, entitled: *Wiretapping and Electronic Surveillance: A Brief Discussion of Pertinent Supreme Court Cases, A Summary and Compilation of Federal State Statutes, and a Selected Legal Bibliography* (1970); *Wiretapping and Electronic Surveillance: A Brief Discussion of Pertinent Supreme Court Cases, A Summary and Compilation of Federal State Statutes, and a Selected Legal Bibliography* (1971); *Wiretapping and Electronic Surveillance: Federal and State Statutes* (1974); *Taps and Bugs: A Compilation of Federal and State Statutes Governing the Interception of Wire and Oral Communications* (1981); *The Interception of Communications: A Legal Overview of Bugs and Taps* (1988); *Wiretapping & Electronic Surveillance: The Electronic Communications Privacy Act and Related Matters* (1992); *Taps, Bugs & Telephony: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping* (1998); *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping* (2001); *id.* (2003); *id.* (2006). It draws most heavily on a report, which remains available and which unlike the present work includes a discussion of the Foreign Intelligence Surveillance Act (FISA), entitled *Privacy: an Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, CRS Rept. 98-326.

As used in this report "electronic eavesdropping" refers to the use of hidden microphones, recorders and any other mechanical or electronic means of capturing ongoing communications, other than wiretapping (tapping into telephone conversations). In previous versions of this report and other earlier writings, it was common to use a more neutral, and consequently preferred, term – electronic surveillance – at least when referring to law enforcement use. Unfortunately, continued use of the term "electronic surveillance" rather than "electronic eavesdropping" risks confusion with forms of surveillance that either have individualistic definitions (*e.g.*, "electronic surveillance" under the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801(f)), that involve surveillance that does not capture conversation (*e.g.*, thermal imaging or electronic tracking devices), or that may or may not capture conversation (*e.g.*, the coverage of video surveillance depends upon the circumstances and the statutory provision question).

Related developments are discussed in CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions*, by Elizabeth B. Bazan; CRS Report RL34693, *Privacy Law and Online Advertising*, by Kathleen Ann Ruane; CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle; CRS Report RL30677, *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, by Patricia Moloney Figliola; and CRS Report RL34409, *Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers*, by Kathleen Ann Ruane.

[2] 4 BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, 169 (1769).

[3] "Eavesdropping is indictable at the common law, not only in England but in our states. It is seldom brought to the attention of the courts, and our books contain too few decisions upon it to enable an author to define it with confidence. . . . It never occupied much space in the law, and it has nearly faded from the legal horizon." 1 BISHOP, COMMENTARIES (continued...)

and telephone, however, state laws outlawing wiretapping or indiscretion by telephone and telegraph operators preserved the spirit of the common law prohibition in this country.

Congress enacted the first federal wiretap statute as a temporary measure to prevent disclosure of government secrets during World War I.[4] Later, it proscribed intercepting and divulging private radio messages in the Radio Act of 1927,[5] but did not immediately reestablish a federal wiretap prohibition. By the time of the landmark Supreme Court decision in *Olmstead*, however, at least forty-one of the forty-eight states had banned wiretapping or forbidden telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or both.[6]

Olmstead was a Seattle bootlegger whose Prohibition Act conviction was the product of a federal wiretap. He challenged his conviction on three grounds, arguing unsuccessfully that the wiretap evidence should have been suppressed as a violation of either his Fourth Amendment rights, his Fifth Amendment privilege against self-incrimination, or the rights implicit in the Washington state statute that outlawed wiretapping.

For a majority of the Court, writing through Chief Justice Taft, Olmstead's Fourth Amendment challenge was doomed by the absence of "an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage[7] for the purposes of making a seizure."[8]

Chief Justice Taft pointed out that Congress was free to provide protection which the Constitution did not.[9] Congress did so in the 1934 Communications Act by expanding the Radio Act's

---

(...continued)

ON THE CRIMINAL LAW, 670 (1882).

[4] 40 Stat.1017-18 (1918)("whoever during the period of governmental operation of the telephone and telegraph systems of the United States . . . shall, without authority and without the knowledge and consent of the other users thereof, except as may be necessary for operation of the service, tap any telegraph or telephone line . . . or whoever being employed in any such telephone or telegraph service shall divulge the contents of any such telephone or telegraph message to any person not duly authorized or entitled the receive the same, shall be fined not exceeding $1,000 or imprisoned for not more than one year or both"); 56 *Cong.Rec.* 10761-765 (1918).

[5] 44 Stat. 1172 (1927)(". . . no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purpose, effect, or meaning of such intercepted message to any person . . .").

[6] *Olmstead v. United States*, 277 U.S. 438, 479-80 n.13 (1928)(Brandeis, J., dissenting). *Olmstead* is remembered most today for the dissents of Holmes and Brandeis, but for four decades it stood for the view that the Fourth Amendment's search and seizure commands did not apply to government wiretapping accomplished without a trespass onto private property.

[7] Curtilage originally meant the land and buildings enclosed by the walls of a castle; in later usage it referred to the barns, stables, garden plots and the like immediately proximate to a dwelling; it is understood in Fourth Amendment parlance to describe that area which "harbors those intimate activities associated with domestic life and the privacies of the home," *United States v. Dunn*, 480 U.S. 294, 301 n.4 (1987).

[8] 277 U.S. at 466. Olmstead had not been compelled to use his phone and so the Court rejected his Fifth Amendment challenge. 277 U.S.C. at 462. Any violation of the Washington state wiretap statute was thought insufficient to warrant the exclusion of evidence, 277 U.S. at 466-68. Justice Holmes in his dissent tersely characterized the conduct of federal wiretappers as "dirty business," 277 U.S. at 470. The dissent of Justice Brandeis observed that the drafters of the Constitution "conferred as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government against privacy of the individual whatever the means employed, must be deemed in violation of the Fourth Amendment," 277 U.S. at 478-79.

[9] "Congress may of course protect the secrecy of telephone messages by making them, when intercepted inadmissible in evidence in federal criminal trials, by direct legislation," 277 U.S. at 465.

proscription against intercepting and divulging radio communications so as to include intercepting and divulging radio or wire communications.[10]

The Federal Communications Act outlawed wiretapping, but it said nothing about the use of machines to surreptitiously record and transmit face to face conversations.[11] In the absence of a statutory ban the number of surreptitious recording cases decided on Fourth Amendment grounds surged and the results began to erode *Olmstead*'s underpinnings.[12]

Erosion, however, came slowly. Initially the Court applied *Olmstead*'s principles to the electronic eavesdropping cases. Thus, the use of a dictaphone to secretly overhear a private conversation in an adjacent office offended no Fourth Amendment precepts, because no physical trespass into the office in which the conversation took place had occurred.[13] Similarly, the absence of a physical trespass precluded Fourth Amendment coverage of the situation where a federal agent secretly recorded his conversation with a defendant held in a commercial laundry in an area open to the public.[14] On the other hand, the Fourth Amendment did reach the government's physical intrusion upon private property during an investigation, as for example when they drove a "spike mike" into the common wall of a row house until it made contact with a heating duct for the home in which the conversation occurred.[15]

The spike mike case presented something of a technical problem, because there was some question whether the spike mike had actually crossed the property line of the defendant's town house when it made contact with the heating duct. The Court declined to rest its decision on the technicalities of local property law, and instead found that the government's conduct had intruded upon privacy of home and hearth in a manner condemned by the Fourth Amendment.[16]

---

[10] 48 Stat. 1103-104 (1934), 47 U.S.C. 605 (1940 ed.). The Act neither expressly condemned law enforcement interceptions nor called for the exclusion of wiretap evidence, but it was read to encompass both, *Nardone v. United States*, 302 U.S. 379 (1937*); Nardone v. United States*, 308 U.S. 321 (1939).

[11] Section 605 did ban the interception and divulgence of radio broadcasts but it did not reach the radio transmission of conversations that were broadcast unbeknownst to all of the parties to the conversation. Late in the game, the FCC supplied a partial solution when it banned the use of licensed radio equipment to overhear or record private conversation without the consent of all the parties involved in the conversation, 31 *Fed.Reg.* 3400 (March 4, 1966), amending then 47 C.F.R. §§2.701, 15.11. The FCC excluded "operations of any law enforcement offices conducted under lawful authority," *id.*

[12] The volume of all Fourth Amendment cases calling for Supreme Court review increased dramatically after *Mapp v. Ohio*, 367 U.S. 643 (1961), acknowledged the application of the Fourth Amendment exclusionary rule to the states.

[13] *Goldman v. United States*, 316 U.S. 129 (1942).

[14] *On Lee v. United States*, 343 U.S. 747 (1952).

[15] *Silverman v. United States*, 365 U.S. 505 (1961).

[16] "The absence of a physical invasion of the petitioner's premises was also a vital factor in the Court's decision in *Olmstead v. United States* . . . . In holding that the wiretapping there did not violate the Fourth Amendment, the Court noted that the insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses. 277 U.S. at 457. There was no entry of the houses or offices of the defendants. 277 U.S. at 464. Relying upon these circumstances, the Court reasoned that the intervening wires are not part of (the defendant's) house or office any more than are the highways along which they are stretched. 277 U.S. at 465.

"Here, by contrast, the officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office – a heating system which was an integral part of the premises occupied by the petitioners, a usurpation that was effected without their knowledge and without their consent. In these circumstances we need not pause to consider whether or not there was a technical trespass under the local property law relating to party walls. Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law . . . .

"The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the (continued...)

Each of these cases focused upon whether a warrantless trespass onto private property had occurred, that is, whether the *means* of conducting a search and seizure had been so unreasonable as to offend the Fourth Amendment. Yet in each case, the object of the search and seizure had been not those tangible papers or effects for which the Fourth Amendment's protection had been traditionally claimed, but an intangible, a conversation. This enlarged view of the Fourth Amendment could hardly be ignored, for "[i]t follows from . . . *Silverman* . . . that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of papers and effects."[17]

Soon thereafter the Court repudiated the notion that the Fourth Amendment's protection was contingent upon some trespass to real property in *Katz v. United States.*[18] Katz was a bookie convicted on the basis of evidence gathered by an electronic listening and recording device set up outside the public telephone booth that Katz used to take and place bets. The Court held that the gateway for Fourth Amendment purposes stood at that point where an individual should to able to expect that his or her privacy would not be subjected to unwarranted governmental intrusion.[19]

One obvious consequence of Fourth Amendment coverage of wiretapping and other forms of electronic eavesdropping is the usual attachment of the Amendment's warrant requirement. To avoid constitutional problems and at the same time preserve wiretapping and other forms of electronic eavesdropping as a law enforcement tool, some of the states established a statutory system under which law enforcement officials could obtain a warrant, or equivalent court order, authorizing wiretapping or electronic eavesdropping.

The Court rejected the constitutional adequacy of one of the more detailed of these state statutory schemes in *Berger v. New York.*[20] The statute was found deficient because of its failure to require:

- a particularized description of the place to be searched;

(...continued)

right of a man to retreat into his own home and there be free from unreasonable governmental intrusion . . . This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard.

"A distinction between the dictaphone employed in Goldman and the spike mike utilized here seemed to the Court of Appeals too fine a one to draw. The court was unwilling to believe that the respective rights are to be measured in fractions of inches. But decision here does not turn upon the technicality of a trespass upon a party wall as a matter of local law. It is based upon the reality of an actual intrusion into a constitutionally protected area. What the Court said long ago bears repeating now: It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. *Boyd v. United States*, 116 U.S. 616, 635. We find no occasion to re-examine Goldman here, but we decline to go beyond it, by even a fraction of an inch," 365 U.S. at 510-12 (internal quotation marks omitted).

[17] *Wong Sun v. United States*, 371 U.S. 471, 485 (1963).

[18] 389 U.S. 347 (1967).

[19] "We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the trespass doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a search and seizure within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance." Later courts seem to prefer the "expectation of privacy" language found in Justice Harlan's concurrence: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable," 389 U.S. at 361.

[20] 388 U.S. 41 (1967).

- a particularized description of the crime to which the search and seizure related;
- a particularized description of the conversation to be seized;
- limitations to prevent general searches;
- termination of the interception when the conversation sought had been seized;
- prompt execution of the order;
- return to the issuing court detailing the items seized; and
- any showing of exigent circumstances to overcome the want of prior notice.[21]

Berger helped persuade Congress to enact Title III of the Omnibus Crime Control and Safe Streets Act of 1968, a comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both activities in general terms but that also permitted federal and state law enforcement officers to use them under strict limitations designed to meet the objections in *Berger*.[22]

A decade later another Supreme Court case persuaded Congress to supplement Title III with a judicially supervised procedure for the use of wiretapping and electronic eavesdropping in foreign intelligence gathering situations. When Congress passed Title III there was some question over the extent of the President's inherent powers to authorize wiretaps – without judicial approval – in national security cases. As a consequence, the issue was simply removed from the Title III scheme.[23] After the Court held that the President's inherent powers were insufficient to excuse warrantless electronic eavesdropping on purely domestic threats to national security,[24] Congress considered it prudent to augment the foreign intelligence gathering authority of the United States with the Foreign Intelligence Security Act of 1978 (FISA).[25] The FISA provides a procedure for judicial review and authorization or denial of wiretapping and other forms of electronic eavesdropping for purposes of foreign intelligence gathering.

Two other Supreme Court cases influenced the development of federal law in the area. In *United States v. Miller*,[26] the Court held that a customer had no Fourth Amendment protected expectation of privacy in the records his bank created concerning his transactions with them. These third party records were therefore available to the government under a subpoena duces tecum rather than a more narrowly circumscribed warrant.[27] In *Smith v. Maryland*,[28] it held that no warrant was required for the state's use of a pen register or trap and trace device, if the device merely identified the telephone numbers for calls made and received from a particular telephone. No

[21] 388 U.S. at 58-60.

[22] 87 Stat. 197, 18 U.S.C. 2510 - 2520 (1970 ed.).

[23] 18 U.S.C. 2511(3)(1970 ed.)("Nothing contained in this chapter or in section 605 of the Communications Act . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. . .").

[24] *United States v. United States District Court*, 407 U.S. 297 (1972).

[25] 92 Stat. 1783, 50 U.S.C. 1801-1862.

[26] 425 U.S. 435, 441-43 (1976).

[27] *Id.* at 44-45.

[28] 442 U.S. 735, 741-46 (1979).

Fourth Amendment search or seizure occurred, the Court held, since the customer had no justifiable expectation of privacy in information which he knew or should have known the telephone company might ordinarily capture for billing or service purposes.[29]

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA).[30] ECPA consists of three parts: a revised Title III;[31] the Stored Communications Act (SCA));[32] and provisions governing the installation and use of trap and trace devices.[33]

Title III: Prohibitions

Unless otherwise provided, Title III outlaws wiretapping and electronic eavesdropping; possession of wiretapping or electronic eavesdropping equipment; use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping; and disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice, 18 U.S.C. 2511. Elsewhere, federal law proscribes:

- unlawful access to stored communications, 18 U.S.C. 2701;
- unlawful use of a pen register or a trap and trace device, 18 U.S.C. 3121; and
- abuse of eavesdropping and search authority or unlawful disclosures under the Foreign Intelligence Surveillance Act, 50 U.S.C. 1809, 1827.

Illegal Wiretapping and Electronic Eavesdropping

At the heart of Title III lies the prohibition against illegal wiretapping and electronic eavesdropping, 18 U.S.C. 2511(1), that bans:

- any person from
- intentionally
- intercepting, or endeavoring to intercept,
- wire, oral or electronic communications
- by using an electronic, mechanical or other device
- unless the conduct is specifically authorized or expressly not covered, *e.g.*
    - one of the parties to the conversation has consented to the interception

[29] *Id.* In *United States v. New York Telephone Co.*, the Court held that the Title III did not apply to the use of pen registers and that federal courts had the power to authorize their installation for law enforcement purposes, 434 U.S. 157, 168 (1977).

[30] 100 Stat. 1848.

[31] 18 U.S.C. 2510-2522.

[32] 18 U.S.C. 2701-2712.

[33] 18 U.S.C. 3121-3126.

- the interception occurs in compliance with a statutorily authorized, (and ordinarily judicially supervised) law enforcement or foreign intelligence gathering interception,
- the interception occurs as part of providing or regulating communication services,
- certain radio broadcasts, and
- in some places, spousal wiretappers.

Person

The prohibition applies to "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."[34]

Intentional

Conduct can only violate Title III if it is done "intentionally," inadvertent conduct is no crime; the offender must have done on purpose those things which are outlawed.[35] He need not be shown to have known, however, that his conduct was unlawful.[36]

Jurisdiction

Subsection 2511(1) contains two interception bars – one, 2511(1)(a), simply outlaws intentional interception; the other, 2511(1)(b), outlaws intentional interception when committed under any of five jurisdictional circumstances with either an implicit or explicit nexus to interstate or foreign commerce.[37] Congress adopted the approach because of concern that its constitutional authority

[34] 18 U.S.C. 2510(6). Although the governmental entities are not subject to criminal liability, as noted *infra*, some courts believe them subject to civil liability under 18 U.S.C. 2520; *Smoot v. United Transportation Union*, 246 F.3d 633, 640-41 (6th Cir. 2001).

[35] "In order to underscore that the inadvertent reception of a protected communication is not a crime, the subcommittee changed the state of mind requirement under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 from 'willful' to 'intentional,'" S.Rept. 541, at 23 (1986); "This provision makes clear that the inadvertent interception of a protected communication is not unlawful under this Act," H.Rept. 99-647, at 48-9 (1986). *See*, *e.g., In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742-43 (4th Cir. 1994); *Lonegan v. Hasty*, 436 F.Supp.2d 419, 429 (E.D.N.Y. 2006). "But the plaintiffs need not produce direct evidence of the intentional interception; for often the only way to prove that a stealthy interception occurred is through circumstantial evidence," *McCann v. Iroquois Memorial Hospital*, 622 F.3d 745, 752 (7th Cir. 2010), citing, *DirectTV v. Webb*, 545 F.3d 837, 844 (9th Cir. 2008).

[36] *Narducci v. Village of Bellwood*, 444 F.Supp. 924, 935 (N.D. Ill. 2006).

[37] "(1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

"(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when – (I) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for (continued...)

might not be sufficient to ban instances of electronic surveillance that bore no discernable connection to interstate commerce or any other of Congress's enumerated constitutional powers. So it enacted a general prohibition, and as a safety precaution, a second provision more tightly tethered to specific jurisdictional factors.[38] The Justice Department has honored that caution by employing subparagraph (b) to prosecute the interception of oral communications, while using subparagraph (a) to prosecute other forms of electronic eavesdropping.[39]

Interception

Interception "means the aural or other acquisition of the contents" of various kinds of communications by means of "electronic, mechanical or other devices."[40] Although logic might suggest that interception occurs only in the place where the communication is captured, the cases indicate that interception occurs as well where the communication begins, is transmitted, or is received.[41] Yet, it does not include instances when an individual simply reads or listens to a previously intercepted communication, regardless of whether additional conduct may implicate the prohibitions on use or disclosure.[42]

Once limited to aural acquisitions, ECPA enlarged the definition of "interception" by adding the words "or other acquisition" so that it is no longer limited to interceptions of communications that

---

(...continued)

the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States," 18 U.S.C. 2511(1)(a),(b).

[38] "Subparagraph (a) establishes a blanket prohibition against the interception of wire communication. Since the facilities used to transmit wire communications form part of the interstate or foreign communications network, Congress has plenary power under the commerce clause to prohibit all interception of such communications whether by wiretapping or otherwise.

"The broad prohibition of subparagraph (a) is also applicable to the interception of oral communications. The interception of such communications, however, does not necessarily interfere with the interstate or foreign commerce network, and the extent of the constitutional power of Congress to prohibit such interception is less clear than in the case of interception of wire communications. . . .

"Therefore, in addition to the broad prohibitions of subparagraph (a), the committee has included subparagraph (b), which relies on accepted jurisdictional bases under the commerce clause, and other provisions of the Constitution to prohibit the interception of oral communications," S.Rept. 90-1097, at 91-2 (1968).

[39] DEPARTMENT OF JUSTICE CRIMINAL RESOURCE MANUAL §9-60.200 at 1050, available at http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/60mcrm.htm#9-60.400. As will be noted in a moment, the statutory definitions of wire and electronic communications contain specific commerce clause elements, but the definition of oral communications does not. Subsequent Supreme Court jurisprudence relating to the breadth of Congress's commerce clause powers indicates that the precautions may have been well advised, *United States v. Lopez*, 514 U.S. 549 (1995) and *United States v. Morrison*, 529 U.S. 598 (2000).

[40] 18 U.S.C. 2510(4). The dictionary definition of "aural" is "of or relating to the ear or to the sense of hearing," MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 76 (10th ed. 1996).

[41] *United States v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006)("an interception occurs where the tapped phone is located and where the law enforcement officers first overheard the call . . . *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992); *accord, United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir. 1997)(concluding that an interception occurs in the jurisdiction where the tapped phone is located, where the second phone in the conversation is located, and where the scanner used to overhear the call is located); *United States v. Denman*, 100 F.3d 399, 403 (5th Cir. 1996)").

[42] *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009)("In reaching this conclusion, we join a number of other circuits that have held that replaying of tapes containing recorded phone conversations does not amount to a new interception in violation of the Wiretap Act"), *citing inter alia, United States v. Hammond*, 286 F.3d 189, 193 (4th Cir. 2002); *Reynolds v. Spears*, 93 F.3d 428, 432-33 (8th Cir. 1996); *United States v. Shields*, 675 F.2d 1152, 1156 (11th Cir. 1982).

can be heard.[43] The change complicates the question of whether the wiretap, stored communications, or trap and trace portions of the ECPA govern the legality of various means of capturing information relating to a communication. The analysis might seem to favor wiretap coverage when it begins with an examination of whether an "interception" has occurred. Yet, there is little consensus over when an interception occurs; that is, whether "interception" as used in section 2511 contemplates surreptitious acquisition, either contemporaneous with transmission, or whether such acquisition may occur anytime before the initial cognitive receipt of the contents by the intended recipient, or under some other conditions.[44]

The USA PATRIOT Act resolved some of the statutory uncertainty concerning voice mail when it removed voice mail from the wiretap coverage of Title III (striking the phrase "and such term includes any electronic storage of such communication" from the definition of "wire communications" in Title III (18 U.S.C. 2510(1)) and added stored *wire* communications to the stored communications coverage of 18 U.S.C. 2703.[45]

Content

The interceptions proscribed in Title III are confined to those that capture a communication's "content," that is, "information concerning [its] substance, purport, or meaning."[46] Trap and trace

[43] S.Rept. 99-541, at 13 (1986)(the "amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication"); *see also,* H.Rept. 99-647, at 34 (1986).

[44] *See, United States v. Szymuszkiewicz*, 622 F.3d 701, 705-706 (7th Cir. 2010)(an employee's surreptitiously programming his supervisor's computer, so that the server forwards duplicates to the employee of all emails sent to the supervisor, constitutes an interception in violation of Title III); *United States v. Councilman*, 418 F.3d 67, 79-80(1st Cir. 2005)(en banc)(service provider's access to email "during transient storage" constitutes "interception"; without deciding whether "interception is limited to acquisition contemporaneous with transmission"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002)(fraudulent access to stored communication does not constitute an "interception"; interception requires access contemporaneous with transmission); *United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998)(unauthorized retrieval and recording of another's voice mail messages constitutes an "interception"); *United States v. Jones*, 451 F.Supp.2d 71, 75 (D.D.C. 2006)(government's acquisition from the phone company of text messages was no interception because there was no contemporaneous access); *Fraser v. National Mutual Insurance Co.*, 135 F.Supp.2d 623, 634-37 (E.D.Pa. 2001)("interception" of email occurs with its unauthorized acquisition prior to initial receipt by its addressee); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461-62 n.7 (5th Cir. 1994)(Congress did not intend for "interception" to apply to email stored on an electronic bulletin board; stored wire communications (voice mail), however, is protected from "interception"); *United States v. Meriwether*, 917 F.2d 955, 959-60 (6th Cir. 1990)(access to stored information through the use of another's pager does not constitute an "interception"); *United States v. Reyes*, 922 F.Supp. 818, 836-37 (S.D.N.Y. 1996)(same); *Wesley College v. Pitts*, 947 F.Supp. 375, 385 (D.Del. 1997)(no "interception" occurs when the contents of electronic communications are acquired unless contemporaneous with their transmission); *Cardinal Health 414, Inc.v. Adams*, 582 F.Supp.2d 967, 979-81 (M.D. Tenn. 2008)(same); *see also*, *Adams v. Battle Creek*, 250 F.3d 980, 982 (6th Cir. 2001)(use of a "clone" or duplicate pager to simultaneously receive the same message as a target pager is an "interception"); *Brown v. Waddell*, 50 F.3d 285, 294 (4th Cir. 1995)(same).

[45] 115 Stat. 283 (2001). Such recourse to the procedures of the Stored Communications Act must still comply with the demands of the Fourth Amendment, *see, United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010)("Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP. The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional").

[46] 18 U.S.C. 2510(8).

devices and pen registers once captured only information relating to the source and addressee of a communication, not its content. That is no longer the case. The "post-cut-through dialed digit features" of contemporary telephone communications now transmit communications in such a manner that the use of ordinary pen register or trap and trace devices will capture both non-content and content.[47] As a consequence, a few courts have held, either as a matter of statutory construction or constitutional necessity, that the authorities must rely on a Title III wiretap order rather than a pen register/trap and trace order if such information will be captured.[48]

By Electronic, Mechanical, or Other Device

The statute does not cover common law "eavesdropping," but only interceptions "by electronic, mechanical or other device."[49] The term includes computers,[50] but it is defined so as not to include hearing aids or extension telephones in normal use (use in the "ordinary course of business").[51] Whether an extension phone has been installed and is being used in the ordinary course of business or in the ordinary course of law enforcement duties, so that it no longer constitutes an interception device for purposes of Title III and comparable state laws has proven a somewhat vexing question.[52]

Although often intertwined with the consent exception discussed below, the question generally turns on the facts in a given case.[53] When the exemption is claimed as a practice in the ordinary

---

[47] "'Post-cut-through dialed digits' are any numbers dialed from a telephone after the call is initially setup or 'cut-through.' Sometimes these digits are other telephone numbers, as when a party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party. Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like. In the latter case, the digits represent communications content; in the former, they are non-content call processing numbers," *In re United States*, 441 F.Supp.2d 816, 818 (S.D. Tex. 2006).

[48] *In re United States for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices*, 515 F.Supp.2d 325, 328-38 (E.D.N.Y. 2007); *In re United States*, 441 F.Supp.2d 816, 818-27 (S.D. Tex. 2006).

[49] 18 U.S.C. 2510(4). *United States v. Jones*, 451 F.Supp.2d 71, 75 (D.D.C. 2006)(government's acquisition from the phone company of text messages was not an interception because it did not involve contemporaneous access and because no electronic, mechanical, or other devices were used).

[50] *United States v. Szymuszkiewicz*, 622 F.3d 701, 707 (7th Cir. 2010)("Thus Szymuszkiewicz acquired the emails by using at least three devices: Infusino's computer (where the rule [directing surreptitious duplication of incoming emails] was set up), the Kansas City server (where the rule caused each message to be duplicated and sent his way), and his own computer (where the messages were received, read, and sometimes stored").

[51] "'[E]lectronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than – (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal," 18 U.S.C. 2510(5).

[52] See the cases cited and commentary in Barnett & Makar, *"In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping*, 10 HASTINGS JOURNAL OF COMMUNICATIONS AND ENTERTAINMENT LAW 715 (1988); *Application to Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§2510 et seq.), Pertaining to Interceptions of Wire Communications*, 58 ALR Fed. 594; *Eavesdropping on Extension Telephone as Invasion of Privacy*, 49 ALR 4th 430.

[53] *E.g., Deal v. Spears*, 780 F.Supp. 618, 623 (W.D.Ark. 1991), *aff'd*, 980 F.2d 1153 (8th Cir. 1992)(employer regularly taped employee calls by means of a device attached to an extension phone; most of the calls were personal and recording and disclosing them served no business purpose).

course of business, the interception must be for a legitimate business reason, it must be routinely conducted, and at least in some circuits employees must be notified that their conversations are being monitored.[54] Similarly, "Congress most likely carved out an exception for law enforcement officials to make clear that the routine and almost universal recording of phone lines by police departments and prisons, as well as other law enforcement institutions, is exempt from the statute."[55] The exception contemplates administrative rather than investigative monitoring,[56] which must nevertheless be justified by a lawful, valid law enforcement concern.[57]

Wire, Oral, or Electronic Communications

An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects, in oversimplified terms – telephone (wire), face to face (oral), and computer (electronic). Thus, silent video surveillance is ordinarily considered beyond ECPA's reach.[58]

Congress used the definitions of the three forms of communications to describe other communications beyond the ECPA's reach as well as those within its grasp. For example, "oral communication" by definition includes only those face to face conversations with respect to which the speakers have a justifiable expectation of privacy.[59] Similarly, "wire communications"

---

[54] *Adams v. Battle Creek*, 250 F.3d 980, 983 (6th Cir. 2001); *Arias v. Mutual Central Alarm Service*, 202 F.3d 553, 558 (2d Cir. 2000); *Berry v. Funk*, 146 F.3d 1003, 1008 (D.C.Cir. 1998); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 741 (4th Cir. 1994). *See also, Hall v. Earthlink Network Inc.*, 396 F.3d 500, 503-04 (2d Cir. 2005) (Internet service provider's receipt and storage of former customer's email after termination of the customer's account was done in ordinary course of business and consequently did not constitute an interception).

Some courts include surreptitious, extension phone interceptions conducted within the family home as part of the "business extension" exception, *Anonymous v. Anonymous*, 558 F.2d 677, 678-79 (2d Cir. 1977); *Scheib v. Grant*, 22 F.3d 149, 154 (7th Cir. 1994); *Newcomb v. Ingle*, 944 F.2d 1534, 1536 (10th Cir. 1991); *contra, United States v. Murdock*, 63 F.3d 1391, 1400 (6th Cir. 1995).

[55] *Adams v. Battle Creek*, 250 F.3d at 984; *see also, United States v. Lewis*, 406 F.3d 11, 18 (1st Cir. 2005); *United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002); *Smith v. U.S.Dept. of Justice*, 251 F.3d 1047, 1049-50 (D.C.Cir. 2001); *United States v. Poyck*, 77 F.3d 285, 292 (9th Cir. 1996); *United States v. Daniels*, 902 F.2d 1238, 1245 (7th Cir. 1990); *United States v. Paul*, 614 F.2d 115, 117 (6th Cir. 1980).

[56] *Amati v. Woodstock*, 176 F.3d 952, 955 (7th Cir. 1999)("Investigation is within the ordinary course of law enforcement, so if 'ordinary' were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent. Since the purpose of the statute was primarily to regulate the use of wiretapping and other electronic surveillance for investigatory purposes, 'ordinary' should not be read so broadly; it is more reasonably interpreted to refer to routine noninvestigative recording of telephone conversations"); *accord, United States v. Lewis*, 416 F.3d at 11; *Colandrea v. Orangetown*, 411 F.Supp.2d 342, 347-48 (S.D.N.Y. 2007).

[57] The exception, however, does not permit a county to record all calls in and out of the offices of county judges merely because a detention center and the judges share a common facility, *Abraham v. Greenville*, 237 F.3d 386, 390 (4th Cir. 2001), nor does it permit jailhouse telephone monitoring of an inmate's confession to a clergyman, *Mockaitis v. Harcleroad*, 104 F.3d 1522, 1530 (9th Cir. 1997). The courts are divided over whether private corrections officials are covered by the law enforcement exception. *Compare, United States v. Faulkner*, 323 F. Supp.2d 1111, 1113-17 (D. Kan. 2004), *aff'd on other grounds*, 439 F.3d 1221 (10th Cir. 2006) (not covered) *with, United States v. Rivera*, 292 F. Supp.2d 838, 842-43 (E.D.Va. 2003) (covered).

[58] *United States v. Larios*, 593 F.3d 82, 90-91 (1st Cir. 2010); *United States v. Falls*, 34 F.3d 674, 679-80 (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536, 538 (9th Cir. 1992); *United States v. Biasucci*, 786 F.2d 505, 508-509 (2d Cir. 1986); *United States v. Torres*, 751 F.2d 875, 880-81 (7th Cir. 1984).

[59] "'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication," 18 U.S.C. 2510(2). *United States v. Larios*, 593 F.3d 82, 92 (1st Cir. 2010)(emphasis in the original but most internal quotation marks and citations omitted)(The "legislative history of this (continued...)

are limited to those that are at some point involve voice communications (i.e., only aural transfers).[60] Radio and data transmissions are generally "electronic communications." The definition includes other forms of information transfer but excludes certain radio transmissions which can be innocently captured without great difficulty.[61] Although it is not a federal crime to intercept radio communications under any number of conditions, the exclusion is not a matter of definition but of special general exemptions, 18 U.S.C. 2511(2)(g), discussed below.

Endeavoring to Intercept

Although the statute condemns attempted wiretapping and electronic eavesdropping ("endeavoring to intercept"), 18 U.S.C. 2511(1), the provisions appear to have escaped use, interest, or comment heretofore, perhaps because the conduct most likely to constitute preparation for an interception – possession of wiretapping equipment – is already a separate crime, 18 U.S.C. 2512, discussed, *infra*.

Exemptions: Consent Interceptions

Consent interceptions are common, controversial and have a history all their own. The early bans on divulging telegraph or telephone messages had a consent exception.[62] The Supreme Court upheld consent interceptions against Fourth Amendment challenge both before and after the enactment of Title III.[63] The argument in favor of consent interceptions has always been essentially that a speaker risks the indiscretion of his listeners and holds no superior legal position simply because a listener elects to record or transmit his statements rather than subsequently memorializing or repeating them.[64] Wiretapping or electronic eavesdropping by either the police

(...continued)

statutory provision shows that Congress intended this definition to parallel the 'reasonable expectation of privacy test' articulated by the Supreme Court in *Katz*. Thus, for Title III to apply, the court must conclude: (1) the defendant had an actual, subjective expectation of privacy – *i.e.*, that his communications were not subject to interception; and (2) the defendant's expectation is one society would objectively consider reasonable. . . . We conclude that the most reasonable reading of the statute is that the meaning of 'oral communication' was intended to parallel *evolving* Fourth Amendment jurisprudence on reasonable expectations of privacy in one's communications"); *Pattee v. Georgia Ports Authority*, 512 F.Supp.2d 1372, 1376-377 (S.D.Ga. 2007).

[60] "'[W]ire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce," 18 U.S.C. 2510(1).

[61] "'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) the radio portion of a cordless telephone communication that is transmitted between the cordless handset and the base unit; (B) any wire or oral communication; (C) any communication made through a tone-only paging device; or (D) any communication from a tracking device (as defined in section 3117 of this title)," 18 U.S.C. 2510(12).

[62] *E.g.*, 47 U.S.C. 605 (1940 ed.).

[63] *On Lee v. United States*, 343 U.S. 747 (1952); *Lopez v. United States*, 373 U.S. 427 (1963); *United States v. White*, 401 U.S. 745 (1971).

[64] *United States v. White*, 401 U.S. at 751 (1971)("Concededly a police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter's Fourth Amendment rights . . . . For constitutional purposes, no different result is required if the agent instead of immediately reporting and transcribing his conversations with defendant, either (1) simultaneously records them with electronic equipment which (continued...)

or anyone else with the consent of at least one party to the conversation is not unlawful under the federal statute.[65] These provisions do no more than shield consent interceptions from the sanctions of federal law; they afford no protection from the sanctions of state law. Many of the states recognize comparable exceptions, but some only permit interception with the consent of *all* parties to a communication.[66]

Under federal law, consent may be either explicitly or implicitly given. For instance, someone who uses a telephone other than his or her own and has been told by the subscriber that conversations over the instrument are recorded has been held to have implicitly consented to interception when using the instrument.[67] This is not to say that subscriber consent alone is sufficient, for it is the parties to the conversation whose privacy is designed to be protected.[68] Although consent may be given in the hopes of leniency from law enforcement officials or as an election between unpalatable alternatives, it must be freely given and not secured coercively.[69]

Private consent interceptions may not be conducted for a criminal or tortious purpose.[70] Some state wiretap laws do not recognize a one party consent exception. There, interception with the consent of but one party to the conversation is a violation of state law. But the federal exception is available as long as the *purpose* of the interception was neither criminal nor tortious – though

---

(...continued)

he is carrying on his person, *Lopez v. United States, supra*; (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency. *On Lee v. United States, supra*. If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks"); *Lopez v. United States* 373 U.S. 427, 439 (1963)("Stripped to its essentials, petitioner's argument amounts to saying that he has a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not susceptible of impeachment. For no other argument can justify excluding an accurate version of a conversation that the agent could testify to from memory. We think the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording").

[65] "(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

"(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," 18 U.S.C. 2511(2)(c), (d).

[66] For citations to state law, *see*, Appendix B.

[67] *United States v. Verdin-Garcia*, 516 F.3d 884, 894-95 (10th Cir. 2008) (inmate use of prison phone); *United States v. Friedman*, 300 F.3d 111, 122-23 (2d Cir. 2002)(same); *United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002) (same); *United States v. Footman*, 215 F.3d 145, 154-55 (1st Cir. 2000) (same); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) (use of landlady's phone); *United States v. Rivera*, 292 F. Supp.2d 838, 843-45 (E.D.Va. 2003) (inmate use of prison phone monitored by private contractors); *see also, United States v. Conley*, 531 F.3d 56, 58-9 (1st Cir. 2008)(explicit consent as a condition for phone privileges).

[68] *Anthony v. United States*, 667 F.2d 870, 876 (10th Cir. 1981).

[69] *United States v. Antoon*, 933 F.2d 200, 203-204 (3d Cir. 1991). *But see*, *O'Ferrell v. United States*, 968 F.Supp. 1519, 1541 (M.D.Ala. 1997) (an individual who spoke to his wife on the telephone after being told by FBI agents who were then executing a search warrant at his place of business that he could only speak to her with the agents listening in consented to the interception, even if FBI's initial search was unconstitutional).

[70] 18 U.S.C. 2511(2)(d); *United States v. Lam*, 271 F.Supp.2d 1182, 1183-184 (N.D.Cal. 2003).

the *means* may have been.[71] At one time, the limitation encompassed interceptions for criminal, tortious, *or* otherwise injurious purposes, but ECPA dropped the reference to injurious purposes for fear that First Amendment values might be threatened should the clause be read to outlaw consent interceptions conducted to embarrass.[72]

Exemptions: Publicly Accessible Radio Communications

Radio communications which can be inadvertently heard or are intended to be heard by the public are likewise exempt. These include not only commercial broadcasts, but ship and aircraft distress signals, tone-only pagers, marine radio and citizen band radio transmissions, and interceptions necessary to identify the source of any transmission, radio or otherwise, disrupting communications satellite broadcasts.[73]

Exemptions: Government Officials

Government officials enjoy an exemption when acting under judicial authority, whether that authority is provided for in Title III for federal and state law enforcement officers acting under a court order;[74] acting in an emergency situation pending issuance of a court order;[75] acting under

---

[71] *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010)("We join the courts that have considered this question, and hold that a cause of action under §2511(2)(d) requires that the interceptor intend to commit a crime or tort independent of the act of recording itself"), citing, *Desnick v. American Broadcasting Co.*, 44 F.3d 1345, 1347-48 (7th Cir. 1995); *Sussman v. American Broadcasting Co*, 186 F.3d 1200, 1201 (9th Cir. 1999).

[72] S.Rept. 99-541, at 17-8 (1986); H.Rept. 99-647, at 39-40 (1986).

[73] "(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person – (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted – (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which – (I) is prohibited by section 633 of the Communications Act of 1934; or (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted," 18 U.S.C. 2511(2)(g).

[74] "*Except as otherwise specifically provided in this chapter* any person who (a) intentionally intercepts . . . ." 18 U.S.C. 2511(1)(emphasis added).

[75] "Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that – (a) an emergency situation exists that involves – (i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime, [–] that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and (b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such (continued...)

the authority of Title III in the case of communications of an intruder in a communications system acting with the approval of the system provider;[76] or acting under the authority of the Foreign Intelligence Surveillance Act,[77] or acting pursuant to the authority according them the use of pen registers and trap and trace devices.[78]

Exemptions: Communication Service Providers

There is a general exemption for those associated with supplying communications services, the telephone company, switchboard operators, and the like. The exemption not only permits improved service and lets the telephone company protect itself against fraud,[79] but it allows for assistance to federal and state officials operating under a judicially supervised interception order,[80] and for the regulatory activities of the Federal Communications Commission.[81]

(...continued)

interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application," 18 U.S.C. 2518(7).

[76] "(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if — (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; (II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser," 18 U.S.C. 2511(2)(i).

[77] "(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act," 18 U.S.C. 2511(2)(e).

[78] "(h) It shall not be unlawful under this chapter – (I) to use a pen register or a trap and trace device (as those terms are defined for the purpose of chapter 206). . . ." 18 U.S.C. 2511(2)(h). Neither the stored communications sections in chapter 121 nor the pen register and trap and trace device in chapter 206 authorize the contemporaneous interception of the contents of a communication. For the citations to state statutes permitting judicial authorization of law enforcement interception of wire, oral or electronic communications, for access to stored electronic communications, and for the use of pen registers and trap and trace devices, *see*, Appendix D.

[79] "(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks . . .

* * *

"(h) It shall not be unlawful under this chapter . . .

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service," 18 U.S.C. 2511(2)(a)(I), (h).

[80] "(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with –

(continued...)

Domestic Exemptions

A few courts recognize a "vicarious consent" exception under which a custodial parent may secretly record the conversations of his or her minor child in the interest of protecting the child.[82] Although rejected by most,[83] a handful of federal courts have held that Title III does not preclude one spouse from wiretapping or electronically eavesdropping upon the other,[84] a result other courts have sometimes reached through the telephone extension exception discussed above.[85]

Illegal Disclosure of Information Obtained by Wiretapping or Electronic Eavesdropping

Although often overlooked, it is also a federal crime to disclose information obtained from illicit wiretapping or electronic eavesdropping, 18 U.S.C. 2511(1)(c):

- any person [who]

(...continued)

> (A) a court order directing such assistance signed by the authorizing judge, or
>
> (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter," 18 U.S.C. 2511(2)(a)(ii).

[81] "(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained," 18 U.S.C. 2511(2)(b).

[82] *Pollock v. Pollock*, 154 F.3d 601, 611 (8th Cir. 1998); *Wagner v. Wagner*, 64 F.Supp.2d 895, 889-901 (D.Minn. 1999); *Campbell v. Price*, 2 F.Supp.2d 1186, 1191-192 (E.D.Ark. 1998); *Thompson v. Dulaney*, 838 F.Supp. 1535, 1544-45 (D.Utah 1993); cf., *Babb v. Eagleton*, 616 F.Supp.2d 1195, 1205-206 (N.D.Okla. 2007).

[83] *Glazner v. Glazner*, 347 F.3d 1212, 1215-16 (11th Cir. 2003); *Heggy v. Heggy*, 944 F.2d 1537, 1539 (10th Cir. 1991); *Kempf v. Kempf*, 868 F.2d 970, 972 (8th Cir. 1989); *Pritchard v. Pritchard*, 732 F.2d 372, 374 (4th Cir. 1984); *United States v. Jones*, 542 F.2d 661, 667 (6th Cir. 1976); *Kratz v. Kratz*, 477 F.Supp. 463, 467-70 (E.D.Pa. 1979); *Heyman v.Heyman*, 548 F.Supp. 1041, 1045-47 (N.D.Ill.1982); *Lombardo v. Lombardo*, 192 F.Supp.2d 885, 809 (N.D.Ill. 2002).

[84] *Simpson v. Simpson*, 490 F.2d 803, 809 (5th Cir. 1974); *Perfit v. Perfit*, 693 F.Supp. 851, 854-56 (C.D.Cal. 1988); *see generally*, *Applicability, in Civil Action, of Provisions of Omnibus Crime Control and Safe Streets Act of 1968 Prohibiting Interception of Communications (18 USCS §2511(1)), to Interception by Spouse, or Spouse's Agent, of Conversations of Other Spouse*, 139 ALR Fed. 517, and the cases discussed therein.

[85] *Anonymous v. Anonymous*, 558 F.2d 677, 678-79 (2d Cir. 1977); *Scheib v. Grant*, 22 F.3d 149, 154 (7th Cir. 1994); *Newcomb v. Ingle*, 944 F.2d 1534, 1536 (10th Cir. 1991); cf., *Babb v. Eagleton*, 616 F.Supp.2d 1195, 1203-205 (N.D. Okla. 2007); *contra, United States v. Murdock*, 63 F.3d 1391, 1400 (6th Cir. 1995).

- intentionally
- discloses or endeavors to disclose to another person
- the contents of any wire, oral, or electronic communication
- having reason to know
- that the information was obtained through the interception of a wire, oral, or electronic communication
- in violation of 18 U.S.C. 2511(1)
- is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper.

This is true of the wiretapper or electronic eavesdropper and of all those who disclose information, that in fact can be traced to a disclosure by the original wiretapper or eavesdropper, with reason to know of the information's illicit origins, except to the extent the First Amendment bans application.[86] The legislative history speaks of a common knowledge limitation on the statute's coverage, but it is not clear whether it refers to common knowledge at the time of interception or at the time of disclosure.[87] By definition, a violation of paragraph 2511(1)(c) requires an earlier unlawful interception under subsection 2511(1). If there is no predicate unlawful interception there can be no violation of paragraph 2511(1)(c).

The results of electronic eavesdropping authorized under Title III may be disclosed and used for law enforcement purposes [88] and for testimonial purposes.[89]

---

[86] *Bartnicki v. Vopper*, 532 U.S. 514, 533-34 (2001), pointed out that the First Amendment right to free speech bars the application of section 2511(1)(c) to the disclosure of illegally intercepted, but lawfully acquired, communications dealing with a matter of unusual public concern. Bartnicki was a union negotiator whose telephone conversations with the union's president were surreptitiously intercepted and recorded a discussion negotiation of a teachers' contract. During the conversation, the possibility of using violence against school board members was mentioned. After the teachers' contract was signed, the unknown wiretapper secretly supplied Yocum, a critic of the union's position, with a copy of the tape. Yocum in turn played it for members of the school board and turned it over to Vopper, a radio talk show host, who played it on his show. Other stations and media outlets published the contents as well. Bartnicki sued Vopper and Yocum for use and disclosure in violation of sections 2511(1)(c) and 2511(1)(d). Vopper and Yocum offered a free speech defense, which the Supreme Court accepted. *But see*, *Quigley v. Rosenthal*, 327 F.3d 1044, 1067-68 (10th Cir. 2003) (denying First Amendment protection for those knowingly involved with interceptors of private matters (not public concerns)); *Boehner v. McDermott*, 484 F.3d 573, 577-81 (D.C.Cir. 2007)(Members of Congress do not have a First Amendment right to disclose unlawful wiretap information in violation of House rules).

[87] "Subparagraphs (c) and (d) prohibit, in turn, the disclosure or use of the contents of any intercepted communication by any person knowing or having reason to know the information was obtained through an interception in violation of this subsection. The disclosure of the contents of an intercepted communication that had already become 'public information' or 'common knowledge' would not be prohibited. The scope of this knowledge required to violate either subparagraph reflects existing law (*Pereira v. United States*, 347 U.S. 1 (1954))," S.Rept. 90-1097, at 93 (1967). The remark may also have been influenced by the high level of intent (willfully rather than intentionally) included in the disclosure provision as reported out.

[88] "Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure," 18 U.S.C. 2517(1).

[89] "Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision (continued...)

It is also a federal crime to disclose, with an intent to obstruct criminal justice, any information derived from lawful police wiretapping or electronic eavesdropping, *i.e.*:

- any person [who]
- intentionally discloses, or endeavors to disclose, to any other person
- the contents of any wire, oral, or electronic communication
- intercepted by means authorized by sections:
    - 2511(2)(a)(ii) (communication service providers, landlords, etc. who assist police setting up wiretaps or electronic eavesdropping devices)
    - 2511(2)(b) (FCC regulatory activity)
    - 2511(2)(c) (police one party consent)
    - 2511(2)(e) (Foreign Intelligence Surveillance Act)
    - 2516 (court-ordered, police wiretapping or electronic surveillance)
    - 2518 (emergency wiretaps or electronic surveillance)
- knowing or having reason to know that
- the information was obtained through the interception of such a communication
- in connection with a criminal investigation
- having obtained or received the information in connection with a criminal investigation
- with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,
- is subject to the same sanctions and remedies as one who illegally wiretaps, 18 U.S.C. 2511(1)(e).[90]

This second disclosure proscription would appear to apply to efforts to obstruct justice by information gleaned from either federal or state police wiretaps. Use of the word "authorized" in

(...continued)

thereof," 18 U.S.C. 2517(3). This does not entitle private litigants to disclosure in the view of at least one court, *In re Motion to Unseal Electronic Surveillance Evidence*, 990 F.2d 1015 (8th Cir. 1993).

When court-ordered interception results in evidence of a crime other than the crime with respect to which the order was issued, the evidence is admissible only upon a judicial finding that it was otherwise secured in compliance with Title III requirements, 18 U.S.C. 2517(5).

[90] When acting with a similar intent, disclosure of the *fact* of authorized federal wiretap or foreign intelligence gathering is proscribed elsewhere in title 18. "Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both."

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both," 18 U.S.C. 2232(d),(e).

conjunction with a list of federal statutes might suggest that the paragraph was only intended to protect wiretap information gathered by federal rather than by federal or state authorities. But most of the cited sections do not "authorize" anything; they simply confine the reach of the statutory prohibitions. And several are as likely to involve state interceptions as federal, *e.g.*, the one-party-consent-under-color-of-law interceptions. Offenders face the criminal and civil liability as those who wiretap.[91]

A third disclosure proscription, 18 U.S.C. 2511(3), applies only to electronic communications service providers to the public "who intentionally divulge the contents of the communication while in transmission" to anyone other than sender and intended recipient.[92] The prohibition comes with its own exemptions for divulgence – when one of the parties to the communications consents, when Title III authorizes disclosure of a court approved interception, when necessary for transmission of the communication, or when it involves inadvertent discovery of information relating to the commission of a crime.[93] Although subsection 2511(3) provides no specific sanctions, violators would presumably be exposed to criminal liability under the general disclosure proscription, 18 U.S.C. 2511(1)(c), and to civil liability under 18 U.S.C. 2520.[94]

Illegal Use of Information Obtained by Unlawful Wiretapping or Electronic Eavesdropping

The prohibition on the use of information secured from illegal wiretapping or electronic eavesdropping mirrors the disclosure provision, 18 U.S.C. 2511(1)(d):

- any person [who]
- intentionally
- uses or endeavors to use to another person
- the contents of any wire, oral, or electronic communication
- having reason to know
- that the information was obtained through the interception of a wire, oral, or electronic communication
- in violation of 18 U.S.C. 2511(1)

[91] 18 U.S.C. 2511(1)(e), (4)(a), 2520(a), (g).

[92] 18 U.S.C. 2511(3)(a) ("Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient").

[93] 18 U.S.C. 2511(3)(b) ("A person or entity providing electronic communication service to the public may divulge the contents of any such communication – (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title; (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency").

[94] Note that subsection 2520(d) establishes a good faith defense that specifically references the prohibition: "A good faith reliance on . . . (3) a good faith determination that section 2511(3). . . of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter. . . ."

- is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper.

The available case law under the use prohibition of paragraph 2511(1)(d) is scant, and the section has rarely been invoked except in conjunction with the disclosure prohibition of paragraph 2511(1)(c). The wording of the two is clearly parallel, the legislative history describes them in the same breath,[95] and they are treated alike for law enforcement purposes.[96]

A few courts had recognized an exception to the disclosure-use bans of subsection 2511(1) where law enforcement officials might disclose or use the results of an illegal interception in which they had played no role.[97]

The criminal and civil liability that attend unlawful use of intercepted communications in violation of paragraph 2511(1)(d) are the same as for unlawful disclosure in violation of paragraphs 2511(1)(c) or 2511(1)(e), or for unlawful interception under paragraphs 2511(1)(a) or 2511(1)(b).[98]

Shipping, Manufacturing, Distributing, Possessing or Advertising Wire, Oral, or Electronic Communication Interception Devices

The proscriptions for possession and trafficking in wiretapping and eavesdropping devices are even more demanding than those that apply to the predicate offense itself. There are exemptions for service providers,[99] government officials and those under contract with the government,[100] but

[95] "Subparagraphs (c) and (d) prohibit, in turn, the disclosure or use of the contents of any intercepted communication by any person knowing or having reason to know the information was obtained through an interception in violation of this subsection," S.Rept. 90-1097, at 93 (1967).

[96] *Compare*, 18 U.S.C. 2517(1)("Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure"), *with* 18 U.S.C. 2517(2)("Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties").

On the other hand, the Supreme Court in *Bartnicki* seemed to parse the constitutionally suspect ban on disclosure from the constitutionally permissible ban on use. *Bartnicki v. Vopper*, 532 U.S. 514, 526-27 (2001)("[T]he naked prohibition against disclosures is fairly characterized as a regulation of pure speech. Unlike the prohibition against the 'use' of the contents of an illegal interception in §2511(1)(d), subsection (c) is not a regulation of conduct").

[97] *Forsyth v. Barr*, 19 F.3d 1527, 1541-545 (5th Cir. 1994); *United States v. Murdock*, 63 F.3d 1391, 1400-403 (6th Cir. 1995); *contra, United States v. Crabtree*, 565 F.3d 887, 889 (4th Cir. 2009); *Berry v. Funk*, 146 F.3d 1003, 1011-13 (D.C.Cir. 1998); *Chandler v. United States Army*, 125 F.3d 1296, 1300-302 (9th Cir. 1997); *In re Grand Jury*, 111 F.3d 1066, 1077 (3d Cir. 1997); *United States v. Vest*, 813 F.2d 477, 481 (1st Cir. 1987); *United States v. Lam*, 271 F.Supp.2d 1182, 1184-187 (N.D.Cal. 2003); *see also*, *United States v. Gray*, 521 F.3d 514, 530 (6th Cir. 2008)(noting that in the Sixth Circuit where the doctrine is recognized it is only available in cases of government use).

[98] 18 U.S.C. 2511(4), 2520(a), (g).

[99] "It shall not be unlawful under this section for – (a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service . . . to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications," 18 U.S.C. 2512(2)(a).

[100] "(2) It shall not be unlawful under this section for . . . (b) an officer, agent, or employee of, or a person under (continued...)

there is no exemption for equipment designed to be used by private individuals, lawfully but surreptitiously.[101]

The three prohibitions in section 2512 present generally common features, declaring that:

- any person who
- intentionally
- either

(a)

- sends through the mail or sends or carries in interstate or foreign commerce
- any electronic, mechanical, or other device
- knowing or having reason to know
- that the design of such device renders it primarily useful
- for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(b)

- manufactures, assembles, possesses, or sells
- any electronic, mechanical, or other device
- knowing or having reason to know
- that the design of such device renders it primarily useful
- for the purpose of the surreptitious interception of wire, oral, or electronic communications, and
- that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(...continued)

contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

"(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device," 18 U.S.C. 2512(2)(b),(3).

[101] *United States v. Spy Factory, Inc.*, 951 F.Supp. 450, 473-75 (S.D.N.Y. 1997); *United States v. Bast*, 495 F.2d 138, 141 (D.C.Cir. 1974).

(c)

- places in any newspaper, magazine, handbill, or other publication or disseminates electronically
- any advertisement of —
  - any electronic, mechanical, or other device
  - knowing or having reason to know
  - that the design of such device renders it primarily useful
  - for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
  - any other electronic, mechanical, or other device
  - where such advertisement promotes the use of such device
  - for the purpose of the surreptitious interception of wire, oral, or electronic communications
- knowing the content of the advertisement and knowing or having reason to know
- that such advertisement will be sent through the mail or transported in interstate or foreign commerce

- shall be imprisoned for not more than five years and/or fined not more than $250,000 (not more than $500,000 for organizations), 18 U.S.C. 2512.

The legislative history lists among the items Congress considered "primarily useful for the purpose of the surreptitious interception of communications: the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler, or cigarette pack."[102]

Questions once raised over whether section 2512 covers equipment designed to permit unauthorized reception of scrambled satellite television signals have been resolved.[103] Each of the circuits to consider the question has now concluded that 2512 outlaws such devices,[104] but simple possession does not give rise to a private cause of action.[105]

---

[102] S.Rept. 90-1097, at 95 (1968).

[103] The two appellate panel decisions that found the devices beyond the bounds of section 2512, *United States v. Herring*, 933 F.2d 932 (11th Cir. 1991) and *United States v. Hux*, 940 F.2d 314 (8th Cir. 1991) were overturned en banc, *United States v. Herring*, 993 F.2d 784, 786 (11th Cir. 1993); *United States v. Davis*, 978 F.2d 415, 416 (8th Cir. 1992).

[104] *United States v. Harrell*, 983 F.2d 36, 37-39 (5th Cir. 1993); *United States v. One Macom Video Cipher II*, 985 F.2d 258, 259-61 (6th Cir. 1993); *United States v. Shriver*, 989 F.2d. 898, 901-06 (7th Cir. 1992); *United States v. Davis*, 978 F.2d 415, 417-20 (8th Cir. 1992); *United States v. Lande*, 968 F.2d 907, 910-11 (9th Cir. 1992); *United States v. McNutt*, 908 F.2d 561, 564-65 (10th Cir. 1990); *United States v. Herring*, 993 F.2d 784, 786-89 (11th Cir. 1991).

[105] *DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1129 (11th Cir. 2004); *DirecTV, Inc. v. Robson*, 420 F.3d 532, 538-39 (5th Cir. 2005)(citing several district court cases that have reached the same conclusion). Proof that the possessor used the device to intercept satellite transmission evidences a violation of section 2511 and exposure to civil liability under section 2520, *DirecTV, Inc. v. Nicholas*, 403 F.3d 223, 227-28 (4th Cir. 2005); *DirecTV, Inc. v. Pepe*, 431 F.3d 162, 169 (3d Cir. 2005).

Title III: Government Access

Each of the prohibitions mentioned above recognizes a procedure for government use notwithstanding the general ban, usually under judicial supervision. Although the influence of the Fourth Amendment is reflected in each of the three chapters – chapter 119 (Title III), chapter 121 (Stored Communications Act), and chapter 206 (pen registers and trap & trace devices) – the procedures of the three are distinctive.

Law Enforcement Wiretapping and Electronic Eavesdropping

Title III exempts federal and state law enforcement officials from its prohibitions on the interception of wire, oral, and electronic communications under three circumstances: (1) pursuant to or in anticipation of a court order,[106] (2) with the consent of one of the parties to the communication;[107] and (3) with respect to the communications of an intruder within an electronic communications system.[108]

To secure a Title III interception order as part of a federal criminal investigation, a senior Justice Department official must approve the application for the court order authorizing the interception of wire or oral communications.[109] The procedure is only available where there is probable cause

---

[106] 18 U.S.C. 2516-2518.

[107] 18 U.S.C. 2511(2)(c).

[108] 18 U.S.C. 2511(2)(i)("It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if – (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; (II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser").
A computer trespasser is a person who: (A) "accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer," 18 U.S.C. 2510(21).

[109] "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of [the predicate offenses]. . ." 18 U.S.C. 2516(1).

Subsection 2516(1) "plainly calls for the prior, informed judgment of enforcement officers desiring court approval for intercept authority, and investigative personnel may not themselves ask a judge for authority to wiretap or eavesdrop. The mature judgment of a particular, responsible Department of Justice official is interposed as a critical precondition of any judicial order," *United States v. Giordano*, 416 U.S. 505, 515-16 (1974). Evidence generated without such senior approval must be suppressed, *id.* at 23. However, "suppression is not warranted . . . when a wiretap application or order either misidentifies a DOJ official who could not legally authorize the wiretap or, . . . identifies no official at all, so long as the record shows that a statutorily designated official actually gave the authorization," *United States v. Gray*, 521 F.3d 514, 526-27 (6th Cir. 2008), *citing in accord, United States v. Callum*, 410 F.3d 571, 576 (9th Cir. 2005); *United States v. Radcliff*, 331 F.3d 1153, 1160-163 (10th Cir. 2003); *United States v. Fudge*, 325 F.3d 910, 918 (7th Cir. 2003).

to believe that the wiretap or electronic eavesdropping will produce evidence of one of a long, but not exhaustive, list of federal crimes,[110] or of the whereabouts of a "fugitive from justice" fleeing from prosecution of one of the offenses on the predicate offense list, 18 U.S.C. 2516(1)(*l*). Any federal prosecutor may approve an application for a court order under section 2518 authorizing the interception of email or other electronic communications and the authority extends to any federal felony rather than more limited list of federal felonies upon which a wiretap or bug must be predicated.[111]

At the state level, the principal prosecuting attorney of a state or any of its political subdivisions may approve an application for an order authorizing wiretapping or electronic eavesdropping based upon probable cause to believe that it will produce evidence of a felony under the state laws covering murder, kidnaping, gambling, robbery, bribery, extortion, drug trafficking, or any other crime dangerous to life, limb or property. State applications, court orders and other procedures must at a minimum be as demanding as federal requirements.[112]

Applications for a court order authorizing wiretapping and electronic surveillance include:

- the identity of the applicant and the official who authorized the application;
- a full and complete statement of the facts including
    - details of the crime,
    - a particular description of the nature, location and place where the interception is to occur,[113]
    - a particular description of the communications to be intercepted, and
    - the identities (if known) of the person committing the offense and of the persons whose communications are to be intercepted;
- a full and complete statement of the alternative investigative techniques used or an explanation of why they would be futile or dangerous;
- a statement of the period of time for which the interception is to be maintained and if it will not terminate upon seizure of the communications sought, a probable cause demonstration that further similar communications are likely to occur;
- a full and complete history of previous interception applications or efforts involving the same parties or places;

[110] The list appears in 18 U.S.C. 2516(1).

[111] "Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony," 18 U.S.C. 2516(3); *e.g., United States v. Benjamin*, 72 F.Supp.2d 161, 189 (W.D.N.Y. 1999).

[112] 18 U.S.C. 2516(2).

[113] Identification of the place where, or facilities over, which the targeted communications are to occur may be excused where the court finds that the suspect has or will take steps to thwart interception, 18 U.S.C. 2518(11), (12).

- in the case of an extension, the results to date or explanation for the want of results; and
- any additional information the judge may require.[114]

Before issuing an order authorizing interception, the court must find:

- probable cause to believe that an individual is, has or is about to commit one or more of the predicate offenses;
- probable cause to believe that the particular communications concerning the crime will be seized as a result of the interception requested;
- that normal investigative procedures have been or are likely to be futile or too dangerous; and
- probable cause to believe that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."[115]

Subsections 2518(4) and (5) demand that any interception order include:

- the identity (if known) of the persons whose conversations are to be intercepted;
- the nature and location of facilities and place covered by the order;
- a particular description of the type of communication to be intercepted and an indication of the crime to which it relates;
- the individual approving the application and the agency executing the order;

---

[114] 18 U.S.C. 2518(1), (2).

[115] 18 U.S.C. 2518(3). Paragraphs 2518(3)(a) and (b) mirror the demands of the Fourth Amendment, *i.e.*, that the court find probable cause to believe that the interception will capture evidence of a specific offense, *United States v. Abu-Jihaad*, 630 F.3d 102, 122 (2d Cir. 2010), *citing, Dalia v. United States*, 441 U.S. 238, 255 (1979). As for the necessity requirement of paragraph 2518(3)(c), the Supreme Court explained in the infancy of Title III that: "[I]t is at once apparent that [Title III] not only limits the crimes for which intercept authority may be obtained but also imposes important preconditions to obtaining any intercept authority at all. Congress legislated in considerable detail in providing for applications and orders authorizing wiretapping and evinced the clear intent to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications. These procedures were not to be routinely employed as the initial step in criminal investigation. Rather, the applicant must state and the court must find that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. §§2518(1)(c) and (3)(c)," *United States v. Giordano*, 416 U.S. 505, 515 (1974).

Thus, "[t]he necessity requirement was intended to ensure that wiretaps are not used as the initial step in a criminal investigation. However, officials need not exhaust every conceivable investigative technique before obtaining a wiretap." *United States v. Forrester*, 616 F.3d 929, 944 (9th Cir. 2010)(internal citations omitted); *see also*, *United States v. Maynard*, 615 F.3d 544, 550 (D.C. Cir. 2010)("[H]aving engaged in an adequate range of investigative endeavors, the government properly sought wiretap permission and was not required to enumerate every technique or opportunity missed or overlooked "); *United States v. Wilson*, 484 F.3d 267, 281 (4th Cir. 2007)(internal citations omitted)("The burden that [2581(3)(c)] imposes on the Government, however, is not great and the adequacy of such a showing is to be tested in a practical and commonsense fashion that does not hamper unduly the investigative powers of law enforcement agents. Although wiretaps are disfavored tools of law enforcement, the Government need not present specific factual information sufficient to establish that it has encountered difficulties in penetrating the criminal enterprise or in gathering evidence such that wiretapping becomes reasonable").

- the period of time during which the interception may be conducted and an indication of whether it may continue after the communication sought has been seized;
- an instruction that the order shall be executed
    - as soon as practicable, and
    - so as to minimize the extent of innocent communication seized; and
- upon request, a direction for the cooperation of communications providers and others necessary or useful for the execution of the order.[116]

Compliance with these procedures may be postponed briefly until after the interception effort has begun, upon the approval of senior Justice Department officials in emergency cases involving organized crime or national security threatening conspiracies or involving the risk of death or serious injury.[117]

The court orders remain in effect only as long as required but not more than 30 days. After 30 days, the court may grant 30 day extensions subject to the procedures required for issuance of the original order.[118] During that time the court may require progress reports at such intervals as it considers appropriate.[119] Intercepted communications are to be recorded and the evidence secured and placed under seal (with the possibility of copies for authorized law enforcement disclosure and use) along with the application and the court's order.[120]

---

[116] 18 U.S.C. 2518(4), (5). Under subsection 2518(5), officers executing an interception order must take efforts to minimize the capture of communications that are outside the scope of the orders, 18 U.S.C. 2518(5); *United States v. De La Cruz Suarez*, 601 F.3d 1202, 1215 (11th Cir. 2010). Whether their efforts are sufficient is matter governed by the circumstances surrounding the interception, *Scott v. United States*, 436 U.S. 128, 135-37 (1978); *United States v. West*, 589 F.3d 936, 939-40 (8th Cir. 2009); *United States v. Yarbrough*, 527 F.3d 1092, 1098 (10th Cir. 2008)("In *United States v. Willis*, this court articulated the proper procedure for determining the reasonableness of governmental efforts to avoid monitoring non-pertinent calls. 890 F.2d 1099, 1102 (10th Cir. 1989). The government must make an initial prima facie showing of reasonable minimization. *Id.* 'Once the government has made a prima facie showing of reasonable minimization, the burden then shifts to the defendant to show more effective minimization could have taken place." *Id.* In determining whether the government has made a prima facie showing of reasonable efforts to minimize the interception of non-pertinent calls, we consider the factors identified by the Supreme Court in *Scott*: (1) whether a large number of the calls are very short, one-time only, or in guarded or coded language; (2) the breadth of the investigation underlying the need for the wiretap; (3) whether the phone is public or private; and (4) whether the non-minimized calls occurred early in the surveillance. 436 U.S. at 140-41. It is also appropriate to consider (5) the extent to which the authorizing judge supervised the ongoing wiretap. *United States v. Lopez*, 300 F.3d 46, 57 (1st Cir. 2002); *United States v. Daly*, 535 F.2d 434, 442 (8th Cir. 1976); *United States v. Vento*, 533 F.2d 838, 853 (3d Cir. 1976)").

[117] 18 U.S.C. 2518(7). An observation made almost a quarter of a century ago remains true: "very little case-law interpretation of the emergency requirement exists," *United States v. Crouch*, 666 F.Supp. 1414, 1416 (N.D. Cal. 1987)(holding that twenty-day-old information indicating the defendants would commit a bank robbery within the next sixty days did not constitute a sufficient emergency to justify invocation of subsection 2518(7)); *but see*, *Nabozny v. Marshall*, 781 F.2d 83, 84-5 (6th Cir. 1986)(holding with respect to a hostage situation "an emergency situation existed within the terms of the statute").

[118] 18 U.S.C. 2518(5).

[119] 18 U.S.C. 2518(6).

[120] 18 U.S.C. 2518(8)(a),(b). Paragraph 2518(8)(a) requires that court ordered interceptions be recorded and that the recording immediately be sealed by the court, upon expiration of the interception authority. The seal or a satisfactory explanation for its absence is a prerequisite to the admissibility of the contents or anything derived from the contents as evidence.

"The 'absence' the Government must satisfactorily explain encompasses not only the total absence of a seal but also the (continued...)

Within 90 days of the expiration of the order those whose communications have been intercepted are entitled to notice, and evidence secured through the intercept may be introduced into evidence with 10 days' advance notice to the parties.[121]

Title III also describes conditions under which information derived from a court ordered interception may be disclosed or otherwise used. It permits disclosure and use for official purposes by:

- other law enforcement officials including foreign officials;[122]
- federal intelligence officers to the extent that it involves foreign intelligence information;[123]
- other American or foreign government officials to the extent that it involves the threat of hostile acts by foreign powers, their agents, or international terrorists.[124]

It also allows witnesses testifying in federal or state proceedings to reveal the results of a Title III tap,[125] provided the intercepted conversation or other communication is not privileged.[126]

Without a Title III order and without offending Title III, authorities may intercept the wire, oral, or electronic communications, it they have the consent of one of the parties to the

(...continued)

absence of a timely applied seal," *United States v. Ojeda Rios,* 495 U.S. 257, 263 (1990). "[T]he 'satisfactory explanation' language in §2518(8)(a) must be understood to require that the Government explain not only why a delay occurred but also why it is excusable," *Id.* at 265; *United States v. Martin*, 618 F.3d 705, 716, 718 (7th Cir. 2010)(some internal citations omitted)("[W]hat should be deemed 'satisfactory' in the context of a statute aimed at preventing government tampering with electronic evidence must depend largely on the statutory objective. A satisfactory explanation must dispel any reasonable suspicion of tampering, and also must be both accurate and believable. Whether the explanation is satisfactory also may depend on the delay in sealing, unique pressure on the Government to obtain a conviction due to particularly notorious charges or defendants, the importance of the recordings to the Government's case and whether the Government has established a procedure for complying with its sealing obligations. . . . *Cf. United States v. Quintero*, 38 F.3d 1317, 1328-330 (3d Cir. 1994) (rejecting the prosecutor's heavy workload as a satisfactory explanation for a sealing delay because to do so 'would be rendering extraordinary that which is ordinary'); *United States v. Carson*, 969 F.2d 1480, 1498 (3d Cir. 1992) (rejecting the need to enhance the audibility of tapes as a satisfactory explanation for a sealing delay because that need was "readily foreseeable and could just as readily become routine").

The section does not preclude use or disclosure other than admissibility of the intercepted contents in judicial proceedings, *United States v. Amanuel*, 615 F.3d 117, 125-28 (2d Cir. 2010)(uphold the admissibility of evidence secured under a warrant based on interceptions that were recorded in violation of section 2518(8)(a)).

[121] 18 U.S.C. 2518(8)(d), (9).

[122] 18 U.S.C. 2517(1), (2), (5), (7).

[123] 18 U.S.C. 2517(6). "'[F]oreign intelligence information,' for purposes of section 2517(6) of this title, means – (A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against – (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or intentional terrorism by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by and intelligence service or network of a foreign power or by an agent of a foreign power; or (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to – (i) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States," 18 U.S.C. 2510(19).

[124] 18 U.S.C. 2518(8).

[125] 18 U.S.C. 2517(3), (5).

[126] 18 U.S.C. 2517(4).

communication.[127] As noted earlier, consent may be either explicitly or implicitly given. For instance, someone who uses a telephone other than his or her own and has been told by the subscriber that conversations over the instrument are recorded has been held to have implicitly consented to interception when using the instrument.[128] This is not to say that subscriber consent alone is sufficient, for it is the parties to the conversation whose privacy is designed to be protected.[129] Although consent may be given in the hopes of leniency from law enforcement officials or as an election between unpalatable alternatives, it must be freely given and not secured coercively.[130]

Little judicial or academic commentary accompanies the narrow "computer trespasser" justification for governmental interception of electronic communications in paragraph 2511(2)(i). The paragraph originated as a temporary provision in the USA PATRIOT Act,[131] and seems designed to enable authorities to track intruders who would surreptitiously use the computer systems of others to cover their trail.[132]

Title III: Consequences of a Violation

Criminal Penalties

Interception, use, or disclosure in violation of Title III is generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.[133] The same penalties apply to the unlawful capture of cell phone and cordless phone conversations, since the Homeland Security Act[134] repealed the reduced

[127] 18 U.S.C. 2511(2)(c).

[128] *United States v. Verdin-Garcia*, 516 F.3d 884, 894-95 (10th Cir. 2008) (inmate use of prison phone); *United States v. Friedman*, 300 F.3d 111, 122-23 (2d Cir. 2002)(same); *United States v. Hammond*, 286 F.3d 189, 192 (4th Cir. 2002) (same); *United States v. Footman*, 215 F.3d 145, 154-55 (1st Cir. 2000) (same); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990) (use of landlady's phone); *United States v. Rivera*, 292 F. Supp.2d 838, 843-45 (E.D.Va. 2003) (inmate use of prison phone monitored by private contractors); *see also*, *United States v. Conley*, 531 F.3d 56, 58-9 (1st Cir. 2008)(explicit consent as a condition for phone privileges).

[129] *Anthony v. United States*, 667 F.2d 870, 876 (10th Cir. 1981).

[130] *United States v. Antoon*, 933 F.2d 200, 203-204 (3d Cir. 1991). *But see, O'Ferrell v. United States*, 968 F.Supp. 1519, 1541 (M.D.Ala. 1997) (an individual who spoke to his wife on the telephone after being told by FBI agents who were then executing a search warrant at his place of business that he could only speak to her with the agents listening in consented to the interception, even if FBI's initial search was unconstitutional).

[131] Section 217, P.L. 107-56, 115 Stat. 291 (2001).

[132] *Implementation of the USA PATRIOT Act: Crime, Terrorism and the Age of Technology: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary*, 109th Cong., 2d sess. 30-1 (2005)(prepared statement of FBI Dep. Ass't Director Steven M. Martinez).

[133] "Except as provided in (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title* or imprisoned not more than five years, or both." 18 U.S.C. 2511(4)(a).

* Section 3559 of title 18 classifies as a felony any offense with a maximum penalty of imprisonment of more than one year; and as a Class A misdemeanor any offense with a maximum penalty of imprisonment set at between six months and one year. Unless Congress clearly rejects the general fine ceilings it provides, section 3571 of title 18 sets the fines for felonies at not more than $250,000 for individuals and not more than $500,000 for organizations, and for class A misdemeanors at not more than $100,000 for individuals and not more than $200,000 for organizations. If there is monetary loss or gain associated with the offense, the offender may alternatively be fined not more than twice the amount of the loss or gain, 18 U.S.C. 3571.

[134] 116 Stat. 2158 (2002).

penalty provisions that at one time applied to the unlawful interceptions using radio scanners and the like.[135] There is a reduced penalty, however, for filching satellite communications as long as the interception is not conducted for criminal, tortious, nor mercenary purposes: unauthorized interceptions are broadly proscribed subject to an exception for unscrambled transmissions[136] and are subject to the general five-year penalty, but interceptions for neither criminal, tortious, nor mercenary purposes subject offenders to only civil punishment.[137] Equipment used to wiretap or eavesdrop in violation of Title III is subject to confiscation by the United States, either in a separate civil proceeding or aa part of the prosecution of the offender.[138]

In addition to exemptions previously mentioned, Title III provides a defense to criminal liability based on good faith.[139]

Civil Liability

Victims of a violation of Title III may be entitled to equitable relief, damages (equal to the greater of actual damages, $100 per day of violation, or $10,000),[140] punitive damages, reasonable

[135] 18 U.S.C. 2511(4)(b)(2000 ed.).

[136] "(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted – (i) to a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purpose of direct or indirect commercial advantage or private financial gain," 18 U.S.C. 2511(4)(b).

[137] "(5)(a)(I) If the communication is – (A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or (B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction. (ii) In an action under this subsection – (A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and (B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

"(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction." 18 U.S.C. 2511(5).

Under 18 U.S.C. 2520, victims may recover the greater of actual damages or statutory damages of not less than $50 and not more than $500 for the first offense; those amounts are increased to $100 and $1000 for subsequent offenses.

[138] 18 U.S.C. 2513 ("Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. . ."); 18 U.S.C. 983(a)(3)(C)("In lieu of, or in addition to, filing a civil forfeiture complaint, the Government may include a forfeiture allegation in a criminal indictment. . .").

[139] "A good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or (3) a good faith determination that section 2511(3) [electronic communications provider authority to disclose content of an electronic communication "(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title; (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency] or 2511(2)(I) [interception of communications of a trespasser in a computer system] of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law," 18 U.S.C. 2520(d).

[140] The $10,000 lump sum for liquidated damages is limited to a single award per victim rather than permitting $10,000 (continued...)

attorney's fees and reasonable litigation costs.[141] A majority of federal courts hold that a court may decline to award damages, attorneys' fees and costs, but a few still consider such awards mandatory.[142] In addition, a majority hold that governmental entities other than the United States may be liable for violations of section 2520[143] and that law enforcement officers enjoy a qualified immunity from suit under section 2520.[144]

The cause of action created in section 2520 is subject to a good faith defense.[145] Efforts to claim the defense by anyone other than government officials or someone working at their direction have been largely unsuccessful.[146]

Civil Liability of the United States

The USA PATRIOT Act authorizes a cause of action against the United States for willful violations of Title III, the Foreign Intelligence Surveillance Act or the provisions governing stored communications in 18 U.S.C. 2701-2712.[147] Successful plaintiffs are entitled to the greater of $10,000 or actual damages, and reasonable litigation costs.[148]

(...continued)

multiples based on the number of violations or the number of types of violations, as long as the violations are "interrelated and time compacted," *Smoot v. United Transportation Union*, 246 F.3d 633, 642-645 (6th Cir. 2001); *Desilets v. Wal-Mart Stores, Inc*., 171 F.3d 711, 713 (1st Cir. 1999).

[141] 18 U.S.C. 2520.

[142] *Compare*, *e.g*., *DirecTV, Inc. v. Barczewski*, 604 F.3d 1004, 1006-1008 (7th Cir. 2010); *DirecTV, Inc. v. Brown*, 371 F.3d 814, 818 (11th Cir. 2004); *Dorris v. Absher*, 179 F.3d, 420, 429-30 (6th Cir. 1999); *Nalley v. Nalley*, 53 F.3d 649, 651-53 (4th Cir. 1995), *Reynolds v. Spears*, 93 F.3d 428, 433 (8th Cir. 1996); *DirecTV, Inc. v. Neznak*, 371 F.Supp.2d 130, 133-34 (D.Conn. 2005) (each concluding that courts have discretion), *with, Rodgers v. Wood*, 910 F.2d 444, 447-49 (7th Cir. 1990) and *Menda Biton v. Menda*, 812 F.Supp. 283, 284 (D. Puerto Rico 1993) (courts have no such discretion) (note that after *Menda*, the First Circuit in *Desilets v. Wal-Mart Stores, Inc.*, 171 F.3d at 716-17 treated as a matter for the trial court's discretion the question of whether the award of plaintiff's attorneys' fees should be reduced when punitive damages have been denied).

[143] *Adams v. Battle Creek*, 250 F.3d 980, 984 (6th Cir. 2001); *Organizacion JD Ltda. v. United States Department of Justice*, 18 F.3d 91, 94-5 (2d Cir. 1994); *Garza v. Bexar Metropolitan Water District*, 639 F.Supp.2d 770, 773-74 (W.D.Tex. 2009); *Connor v. Tate*, 130 F.Supp.2d 1370, 1374 (N.D.Ga. 2001); *Dorris v. Absher*, 959 F.Supp. 813, 820 (M.D.Tenn. 1997), *aff'd/rev'd in part on other grounds*, 179 F.3d 420 (6th Cir. 1999); *PBA Local No. 38 v. Woodbridge Police Department*, 832 F.Supp. 808, 822-23 (D.N.J. 1993) (each concluding that governmental entities may be held liable); *contra, Abbott v. Winthrop Harbor*, 205 F.3d 976, 980 (7th Cir. 2000); *Amati v. Woodstock*, 176 F.3d 952, 956 (7th Cir. 1999).

[144] *Narducci v. Moore*, 572 F.3d 313, 323 (7th Cir. 2009); *Tapley v. Collins*, 211 F.3d 1210, 1216 (11th Cir. 2000); *Blake v. Wright*, 179 F.3d 1003, 1011-13(6th Cir. 1999); *Babb v. Eagleton*, 614 F.Supp.2d 1232, 1237-238 (N.D.Okla. 2008); *contra, Berry v. Funk*, 146 F.3d 1003, 1013 (D.C.Cir. 1998); *see generally*, *Qualified Immunity as Defense in Suit Under Federal Wiretap Act (18 U.S.C.A. §§2510 et seq.)*, 178 ALR FED. 1.

[145] 18 U.S.C. 2520(d) ("A good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or (3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law").

[146] *Williams v. Poulos*, 11 F.3d 271, 285 (1st Cir. 1993); *United States v. Wuliger*, 981 F.2d 1497, 1507 (6th Cir. 1992); *Rice v. Rice*, 951 F.2d 942, 944-45 (8th Cir. 1991); *but see, McCready v. eBay*, 453 F.3d 882, 892 (7th Cir. 2006).

[147] 18 U.S.C. 2712.

[148] 18 U.S.C. 2712(a).

Administrative Action

Upon a judicial or administrative finding of a Title III violation suggesting possible intentional or willful misconduct on the part of a federal officer or employee, the federal agency or department involved may institute disciplinary action. It is required to explain to its Inspector General's office if it declines to do so.[149]

Attorney Discipline

At one time, the American Bar Association (ABA) considered it ethical misconduct for an attorney to intercept or record a conversation without the consent of all of the parties to the conversation, ABA Formal Op. 337 (1974). The reaction of state regulatory authorities with the power to discipline professional misconduct was mixed. Some agreed with the ABA.[150] Some agreed with the ABA, but expanded the circumstances under which recording could be conducted within ethical bounds.[151] Some disagreed with the ABA view.[152] The ABA has since repudiated its

[149] "If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination," 18 U.S.C. 2520(f).

[150] *Ala. Opinion 84-22* (1984); *People v. Smith*, 778 P.2d 685, 686, 687 (Colo. 1989); *Haw. Formal Opinion No. 30* (1988); *Ind.State Bar Ass'n Op.No.1* (2000); *Iowa State Bar Ass'n v. Mollman*, 488 N.W.2d 168, 169-70, 171-72 (Iowa 1992); *Mo.Advisory Comm. Op. Misc. 30* (1978); *Tex.Stat.Bar Op. 514* (1996); *Va. LEO #1635* (1995), *Va. LEO #1324*; *Gunter v. Virginia State Bar*, 238 Va. 617, 621-22, 385 S.E.2d 597, 600 (1989).

The federal courts seem to have been in accord, *Parrott v. Wilson*, 707 F.2d 1262 (11th Cir. 1983); *Moody v. IRS*, 654 F.2d 795 (D.C.Cir. 1981); *Ward v. Maritz, Inc*., 156 F.R.D. 592 (D.N.J. 1994); *Wilson v. Lamb*, 125 F.R.D. 142 (E.D.Ky. 1989); *Haigh V. Matsushita Electric Corp*., 676 F.Supp. 1332 (E.D.Va. 1987).

[151] *Ariz. Opinion No. 95-03* (1995); *Alaska Bar Ass'n Eth.Comm. Ethics Opinions No. 95-5 (1995) and No. 91-4* (1991); *Idaho Formal Opinion 130* (1989); *Kan.Bar.Ass'n Opinion 96-9* (1997); *Ky.Opinion E-279* (1984); *Minn.Law.Prof. Resp.Bd. Opinion No. 18* (1996); *Ohio Bd.Com.Griev.Disp. Opinion No. 97-3* (1997); *S.C. Ethics Advisory Opinion 92-17* (1992); *Tenn.Bd.Prof.Resp. Formal Ethics Opinion No. 86-F-14(a)* (1986).

[152] *D.C. Opinion No. 229* (1992) (recording was not unethical because it occurred under circumstances in which the uninformed party should have anticipated that the conversation would be recorded or otherwise memorialized); *Mississippi Bar v. Attorney ST*., 621 So.2d 229 (Miss. 1993)(context of the circumstances test); *Conn.Bar Ass'n Op. 98-9* (1998)(same); *Mich.State Bar Op. RI-309* (1998)(same); *Me.State Bar Op.No. 168* (1999)(same); *N.M.Opinion 1996-2* (1996)(members of the bar are advised that there are no clear guidelines and that the prudent attorney avoids surreptitious recording); *N.C. RPC 171* (1994)(lawyers are encouraged to disclose to the other lawyer that a conversation is being tape recorded); *Okla.Bar Ass'n Opinion* 307 (1994)(a lawyer may secretly recording his or her conversations without the knowledge or consent of other parties to the conversation unless the recording is unlawful or in violation of some ethical standard involving more than simply recording); *Ore.State Bar Ass'n Formal Opinion No. 1991-74* (1991) (an attorney with one party consent he or she may record a telephone conversation "in absence of conduct which would reasonably lead an individual to believe that no recording would be made"); *Utah State Bar Ethics Advisory Opinion No. 96-04* (1996) ("recording conversations to which an attorney is a party without prior disclosure to the other parties is not unethical when the act, considered within the context of the circumstances, does not involve dishonesty, fraud, deceit or misrepresentation"); *Wis.Opinion E-94-5* ("whether the secret recording of a telephone conversation by a lawyer involves 'dishonesty, fraud, deceit or misrepresentation' under SCR 20:8.4(c) depends upon all the circumstances operating at the time"). In New York, the question of whether an attorney's surreptitiously recording conversations is ethically suspect is determined by locality, compare, *Ass'n of the Bar of City of N.Y. Formal Opinion No. 1995-10* (1995)(secret recording is per se unethical), with, *N.Y.County Lawyer's Ass'n Opinion No. 696* (1993)(secret recording is not per se unethical).

earlier position, ABA Formal Op. 01-422 (2001). Attorneys who engage in *unlawful* wiretapping or electronic eavesdropping will remain subject to professional discipline in every jurisdiction;[153] in light of the ABA's change of position, courts and bar associations have had varied reactions to *lawful* wiretapping or electronic eavesdropping by members of the bar.[154]

Exclusion of Evidence

When the federal wiretap statute prohibits disclosure, the information is inadmissible as evidence before any federal, state, or local tribunal or authority, 18 U.S.C. 2515.[155] Individuals whose conversations have been intercepted or against whom the interception was directed[156] have standing to claim the benefits of the section 2515 exclusionary rule through a motion to suppress under 18 U.S.C. 2518(10)(a). Paragraph 2518(10)(a) bars admission as long as the evidence is the product of (1) an unlawful interception, (2) an interception authorized by a facially insufficient court order, or (3) an interception executed in manner substantially contrary to the order authorizing the interception. Mere technical noncompliance is not enough; the defect must be of a nature that substantially undermines the regime of court-supervised interception for law enforcement purposes.[157]

---

[153] *Cf., Nissan Motor Co., Ltd. v. Nissan Computer Corp*., 180 F.Supp.2d 1089, 1095-97 (C.D.Cal. 2002).

[154] *E.g., State v. Murtagh*, 169 P.3d 602, 617-18 (Alaska 2007)("undisclosed recording is not unethical"); *In re Crossen*, 450 Mass. 533, 558, 880 N.E.2d 352, 372 (2008) (undisclosed recording was unethical where it was part of scheme to coerce or manufacture testimony against the judge presiding over pending litigation); *Midwest Motor Sports v. Arctic Cat Sales, Inc*., 347 F.3d 693, 699 (8th Cir. 2003) (citing *ABA Comm. on Ethics and Prof'l Responsibility*, Formal Op. 01-422, which states that recording without consent should be prohibited when circumstances make it unethical); *United States v. Smallwood*, 365 F. Supp.2d 689, 697-98 (E.D. Va. 2005) (holding that a lawyer cannot ethically record a conversation without the consent of all parties, even though doing so is not illegal under Virginia law). Declaring the new ABA opinion to be an "overcorrection," one bar association explained that secret taping should not be routine practice, but that it should be permitted if it advances a "societal good." *Ass'n of the Bar of the City of New York Formal Opinion No. 2003-02* (2003). For a New York state bar opinion employing a similar line of reasoning, *see, Mena v. Key Food Stores Co-operative, Inc*., 758 N.Y.S.2d 246, 247-50 (N.Y. Sup. Ct. 2003) (conduct of attorney who obtained a private investigator's services for a client and instructed the client on the use of recording equipment held *not* to warrant severe sanctions, because there was a compelling public interest in exposing the racial discrimination that was the subject of the secret recordings); *see also*, *S.C. Bar Ethics Advisory Op. 08-13* (Nov. 14, 2008)(noting that the S.C. ethical prohibition on undisclosed recording by attorneys, based on the earlier ABA opinion, had not been withdrawn); *Tex. Ethics Op.* 575 (Nov. 2006)(undisclosed recording by an attorney is not a per se violation of the Texas Disciplinary Rules of Professional Conduct); *Mo. Formal Advisory Op. 123* (Mar. 8, 2006)(agreeing with ABA Formal Opinion 01-422).

[155] "Whenever any *wire or oral communication* has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter," 18 U.S.C. 2515 (emphasis added); *United States v. Chavez*, 416 U.S. 562, 570 (1974); *United States v. Lnu*, 575 F.3d 298, 301 (3d Cir. 2009); *United States v. Lam*, 271 F.Supp.2d 1182, 1183-184 (N.D.Cal. 2003). Note that suppression does not extend to unlawfully intercepted *electronic* communications, *United States v. Steiger*, 318 F.3d 1039, 1050-52 (11th Cir. 2003); *United States v. Jones*, 364 F. Supp.2d 1303, 1308-09 (D.Utah 2005); nor does it extend to evidence secured in violation the pen register/trap and trace provisions, *United States v. German*, 486 F.3d 849, 852-53 (5th Cir. 2007).

[156] 18 U.S.C. 2510(11)("'aggrieved person' means a person who was a party to any an intercepted wire, oral, or electronic communication or a person against whom the interception was directed"); *United States v. Gonzales*, 412 F.3d 1102, 1115-117 (9th Cir. 2005).

[157] *United States v. Williams*, 124 F.3d 411, 426 (3d Cir. 1997)("The Supreme Court has explained the relationship between these two provisions. In *United States v. Giordano*, 416 U.S. 505 (1974), the Court wrote that 'what disclosures are forbidden under 2515 and we subject to motions to suppress is . . . governed by 2518(10)(a).' Thus, evidence may be suppressed only if one of the grounds set out in 2518(10)(a) is met. Moreover not every failure to (continued...)

Although the Supreme Court has held that section 2515 may require suppression in instances where the Fourth Amendment exclusionary rule would not,[158] some of the lower courts have recognized the applicability of the good faith exception to the Fourth Amendment exclusionary rule in section 2515 cases.[159] Other courts have held, moreover, that the fruits of an unlawful wiretapping or electronic eavesdropping may be used for impeachment purposes.[160]

The admissibility of tapes or transcripts of tapes of intercepted conversations raise a number of questions quite apart from the legality of the interception. As a consequence of the prerequisites required for admission, privately recorded conversations are more likely to be found inadmissible than those recorded by government officials. Admissibility will require the party moving for admission to show that the tapes or transcripts are accurate, authentic and trustworthy.[161] For some courts this demands a showing that, "(1) the recording device was capable of recording the events offered in evidence; (2) the operator was competent to operate the device; (3) the recording is authentic and correct; (4) changes, additions, or deletions have not been made in the recording; (5) the recording has been preserved in a manner that is shown to the court; (6) the speakers on the tape are identified; and (7) the conversation elicited was made voluntarily and in good faith, without any kind of inducement."[162]

(...continued)

comply fully with any requirement provided in Title III would render the interception of wire or oral communications unlawful under 2518(10)(a)(I). *United States v. Donovan*, 429 U.S. 413, 433 (1977), quoting, *United States v. Chavez*, 416 U.S. 562 (1974). Rather suppression is mandated only for a failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device, *Donovan*, 429 U.S. at 433-34, quoting, *Girodano*, 416 U.S. at 527"); *see also*, *United States v. Lopez*, 300 F.3d 46, 55-6 (1st Cir. 2002); *United States v. Staffeldt*, 451 F.3d 578, 582-85 (9th Cir. 2006); *United States v. Gray*, 521 F.3d 514, 522 (6th Cir. 2008). This is the case even where the court is clearly troubled by the government's failure to comply with the requirements of Title III, *United States v. Callum*, 410 F.3d 571, 579 (9th Cir. 2005)("Under the force of precedent, we uphold the challenged wiretap applications and orders. Still, we note that the Department of Justice and its officers did not cover themselves with glory in obtaining the wiretap orders at issue in this case. Title III is an exacting statute obviously meant to be followed punctiliously, yet the officers repeatedly ignored its clear requirements").

[158] *Gelbard v. United States*, 408 U.S. 41, 52 (1972).

[159] *United States v. Moore*, 41 F.3d 370, 376 (8th Cir. 1994); *United States v. Ambrosio*, 898 F.Supp. 177, 187 (S.D.N.Y. 1995); *United States v. Malelzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988); *United States v. Mullen*, 451 F.Supp.2d 509, 530-31 (W.D.N.Y. 2006); *contra, United States v. Rice*, 478 F.3d 704, 711-14 (6th Cir. 2007).

Gelbard held that a grand jury witness might claim the protection of section 2515 through a refusal to answer questions based upon an unlawful wiretap notwithstanding the fact that the Fourth Amendment exclusionary rule does not apply in grand jury proceedings. *Gelbard*, 408 U.S. at 51-52. The good faith exception to the Fourth Amendment exclusionary rule permits the admission of evidence secured in violation of the Fourth Amendment, if the officers responsible for the breach were acting in good faith reliance upon the apparent authority of a search warrant or some like condition negating the remedial force of the rule, *United States v. Leon*, 468 U.S. 897, 909 (1984).

[160] *Culbertson v. Culbertson*, 143 F.3d 825, 827-28 (4th Cir. 1998); *United States v. Echavarria-Olarte*, 904 F.2d 1391 (9th Cir. 1990); *United States v. Vest*, 813 F.2d 477, 484 (1st Cir. 1987); cf., *United States v. Crabtree*, 565 F.3d 887, 891-92 (4th Cir. 2009)(noting that the Circuit's recognition of admissibility for impeachment purposes does not require recognition of a clean hands exception under which the government may admit introduce illegal wiretap evidence as long as it was not involved in the illegal interception).

[161] *United States v. Thompson*, 130 F.3d 676, 683 (5th Cir. 1997); *United States v. Panaro*, 241 F.3d 1104, 1111 (9th Cir. 2001); *United States v. Smith*, 242 F.3d 737, 741 (7th Cir. 2001).

[162] *United States v. Webster*, 84 F.3d 1056, 1064 (8th Cir. 1996); *United States v. Green*, 175 F.3d 822, 830 n.3 (10th Cir. 1999); *United States v. Green*, 324 F.3d 375, 379 (5th Cir. 2003)(citing 4 of the 7 factors); cf., *United States v. Calderin-Rodriguez*, 244 F.3d 977, 986-87 (8th Cir. 2001). These seven factors have been fairly widely cited since they were first announced in *United States v. McKeever*, 169 F.Supp. 426, 430 (S.D.N.Y. 1958), *rev'd on other grounds*, 271 F.2d 669 (2d Cir. 1959). They are a bit formalistic for some courts who endorse a more ad hoc approach to the (continued...)

Stored Electronic Communications (SCA)

SCA: Prohibitions

In its original form Title III was ill-suited to ensure the privacy of those varieties of modern communications which are equally vulnerable to intrusion when they are at rest as when they are in transmission. Surreptitious "access" is as least as great a threat as surreptitious "interception" to the patrons of electronic mail (email), electronic bulletin boards, voice mail, pagers, and remote computer storage.

Accordingly, ECPA, in the Stored Communications Act (SCA), bans surreptitious access to communications at rest, although it does so beyond the confines that apply to interception, 18 U.S.C. 2701 - 2711. These separate provisions afford protection for email, voice mail, and other electronic communications only somewhat akin to that available for telephone and face to face conversations under 18 U.S.C. 2510-2522. The SCA has two sets of proscriptions: a general prohibition and a second applicable to only certain communications providers. The general proscription makes it a federal crime to:

- intentionally
- either
    - access without authorization or
    - exceed an authorization to access
- a facility through which an electronic communication service is provided
- and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system, 18 U.S.C. 2701(a).[163]

The prohibition extends only to "intentional" violations, that is, violations where the defendant had as a conscious objective the forbidden conduct and proscribed result.[164] The offense has three essential components: access, to a facility through which service is supplied, and consequences

(...continued)

assessment of whether the admission of what purports to be a taped conversation will introduce fraud or confusion into the court, *e.g., Stringel v. Methodist Hosp. of Indiana, Inc*., 89 F.3d 415, 420 (7th Cir. 1996)(McKeever "sets out a rather formal, seven step checklist for the authentication of tape recordings, and we have looked to some of the features [in the past]"); *United States v. White*, 116 F.3d 903, 921 (D.C.Cir. 1997)("tapes may be authenticated by testimony describing the process or system that created the tape or by testimony from parties to the conversation affirming that the tapes contained an accurate record of what was said"); *United States v. Tropeano*, 252 F.3d 653, 661 (2d Cir. 2001)("[T]his Circuit has never expressly adopted a rigid standard for determining the admissibility of tape recordings"); *United States v. Westmoreland*, 312 F.3d 302, 310-11 (7th Cir. 2002); *United States v. Dawson*, 425 F.3d 389, 393 (7th Cir. 2005)("But there are no rigid rules, such as chain of custody, for authentication; all that is required is adequate evidence of genuineness. (There are such rules for electronic surveillance governed by Title III, but Title III is inapplicable to conversations that, as here, are recorded with the consent of one of the participants)").

[163] *E.g.*, *State Analysis, Inc. v. American Finacial Services Ass'n*, 621 F.Supp.2d 309, 317-18 (E.D.Va. 2009); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F.Supp.2d 548, 555 (S.D.N.Y. 2008).

[164] *KLA-Tencor Corp. v. Murphy*, 717 F.Supp.2d 895, 905 (N.D.Cal. 2010); *Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 976 (M.D.Tenn. 2008).

(obtain, alter, prevent access to a wire or electronic communication). The first requires either unauthorized access or access in excess of authorization. The third requires either acquisition or alteration of an electronic communication or denial of access to it. The courts have encountered little difficulty in determining whether a defendant's conduct constitutes obtaining, altering, or preventing access to a communication. They have divided, however, over cases in which the defendant was granted access to a communication but used access for the purposes other than that for which it was authorized.[165] The question is less divisive when the grant of access is expressly limited[166] or when an individual with authorized access provides an outsider with his user name and password.[167]

The "facility through which an electronic communication service is provided" need not be one made available to the public; but includes as well facilities through which a private employer provides electronic communication services to his employees.[168]

The section only protects communications while "in electronic storage" in a facility through which electronic communications service is provided. "Electronic storage" is defined to encompass temporary, intermediate storage incidental to transmission as well as backup storage.[169] The definition is not always easily applied.[170]

---

[165] *Penrose Computer Marketgroup, Inc. v. Camin*, 682 F.Supp.2d 202, 210-12 (N.D.N.Y. 2010) citing cases on each side of the debate including cases under the Computer Fraud and Abuse Act (18 U.S.C. 1030) where the "access" terms are used, *e.g.*, *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1125 (W.D.Wash. 2000)("[T]he authority of the plaintiff's . . . employees ended when they allegedly became agents of the defendant [although still employed by the plaintiff]. . . [T]hey lost their authorization and were without authorization when they allegedly obtained and sent the proprietary information to the defendant via email"); *Ass'n of Machinists and Aerospace Workers v. Werner*, 390 F.Supp.2d 479, 496 (D.Md. 2005)("Because section 2701 prohibits only unauthorized access and not the misappropriation or disclosure of information, there is no violation of section 2701 for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access").

[166] *KLA-Tencor Corp. v. Murphy*, 717 F.Supp.2d 895, 905-906 (N.D.Cal. 2010)("Finally, plaintiff has not established that Chen's conduct [of deleting her e-mails in her employer's system] was unauthorized. Plaintiff asserts that Chen was 'without authorization or exceeded authorization to access these e-mails on KT's e-mail server in [her] last days at KT because [she] did not have any legitimate business reasons for doing so and [is] prohibited, as a condition of their employment, from unauthorized use of KT information.' However, this claim is not supported by the evidence. As an initial matter, it appears that employees were generally authorized to use their own e-mail account. . . . The employment agreements cited by plaintiff in its motion only restrict use of *confidential* information, and plaintiff has provided no evidence that the contents of the deleted e-mails were confidential or that deleting e-mails would constitute 'use.' In addition, Chen states that there was no company policy prohibiting her from deleting her own e-mail").

In a case under the Computer Fraud and Abuse Act, that might as easily have been brought under the SCA, however, the court held that "if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law 'that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]' [and consequently is unconstitutionally vague]," *United States v. Drew*, 259 F.R.D. 449, 467 (C.D.Cal. 2009).

[167] *Cardinal Health 414, Inc. v. Adams*, 582 F.Supp. 967, 977 (M.D. Tenn. 2008)("Adams used the log-in information for another person, a former co-worker, to spy on the activities of his former company. On these facts, to argue that continued access was 'authorized' is absurd"); *see also, State Analysis, Inc. v. American Financial Services Assoc.*, 621 F.Supp.2d 309, 318 (E.D.Va. 2009).

[168] *Devine v. Kapasi*, 729 F.Supp.2d 1024, 1027-28 (N.D.Ill. 2010), *citing, Fraser v. Nationwide Mutual Ins. Co*, 352 F.3d 107, 115 (3d Cir. 2003).

[169] 18 U.S.C. 2711(1)("As used in this chapter [18 U.S.C. 2701-2712] – (1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section"); 18 U.S.C. 2510(17)("'electronic storage' means – (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication").

Section 2701's prohibitions yield to several exceptions and defenses. First, the section itself declares that:

> Subsection (a) of this section does not apply with respect to conduct authorized –
>
> (1) by the person or entity providing a wire or electronic communications service;
>
> (2) by a user of that service with respect to a communication of or intended for that user; or
>
> (3) in section 2703 [requirements for government access],
>
> 2704 [backup preservation] or
>
> 2518 [court ordered wiretapping or electronic eavesdropping] of this title. 18 U.S.C. 2701(c).

Second, there are the good faith defenses provided by section 2707:

> A good faith reliance on –
>
> (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title) [relating to an official request for a service provider preserve evidence];
>
> (2) a request of an investigative or law enforcement officer under section 2518(7) of this title [relating to emergency wiretapping and electronic eavesdropping]; or
>
> (3) a good faith determination that section 2511(3) of this title [relating to the circumstances under which an electronic communications provider may divulge the contents of communication][171] permitted the conduct complained of

---

(...continued)

[170] *See e.g., KLA-Tencor Corp. v. Murphy*, 717 F.Supp.2d 895, 904-905 (N.D.Cal. 2010)("As an initial matter, it is not clear to the court that e-mails on KT's server were in 'electronic storage' within the meaning of the SCA. In *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004), the Ninth Circuit held that messages remaining on an ISP's server after delivery could fall within the SCA. The court found that '[a]n obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again-if, for example, the message is accidentally erased from the user's own computer.' *Id*. However, 'the mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose' *Id*. at 1076. The court noted that there would be instances where an ISP could hold messages not in electronic storage, such as 'messages a user has flagged for deletion from the server.' *Id*. In an apparent attempt to mirror *Theofel* language, plaintiff suggests that its server's storage of e-mail has a backup purpose because a user could 'download them again when, for instance, his or her e-mails are accidentally deleted from the computer while working in an offline mode.' Gurule SJ Decl. ¶ 7. However, plaintiff also explains that the server's software 'is configured to synchronize a user's e-mail account so that the account contains the same set of e-mails regardless of where it is accessed.' *Id.* ¶ 10. It seems to the court that these two purposes cannot coexist. Either the server is linked to the computer and flags for deletion a message that is deleted on the computer, or it acts as a backup and would not automatically delete messages that are deleted on a computer. Under either theory, plaintiff's SCA claim fails. Even if the system's operation is as plaintiff describes, the fact that automatic deletion does not occur in the specific situation of a message being deleted while the computer is offline does not establish that the server stores e-mails for the purposes of backup protection rather than only for purpose of synchronization").

[171] "(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication– (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title; (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency," 18 U.S.C. 2511(3).

> is a complete defense to any civil or criminal action brought under this chapter or any other law. 18 U.S.C. 2707(e).

Third, there is the general immunity from civil liability afforded providers under subsection 2703(e):

> [N]o cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

A second set of prohibitions appears in section 2702 and supplements those in section 2701. Section 2702 bans the disclosure of the content of electronic communications and records relating to them by those who provide the public with electronic communication service or remote computing service. The section forbids providers to disclose the content of certain communications to anyone[172] or to disclose related records to governmental entities.[173]

Public electronic communication service (ECS) providers to the public must keep confidential the content of any "communication while in electronic storage by that service."[174] Public remote computer service (RCS) providers must keep confidential the content of "any communication which is carried or maintained on that service – (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[175]

Both sets of providers must keep confidential any "record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any government entity."[176]

Section 2702 comes with its own set of exceptions which permit disclosure of the contents of a communication:

> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> (2) as otherwise authorized in section 2517 [relating to disclosures permitted under Title III], 2511(2)(a)[relating to provider disclosures permitted under Title III for protection of provider property or incidental to service], or 2703 [relating to required provider disclosures pursuant to governmental authority] of this title;
>
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or *the subscriber in the case of remote computing service*;

[172] 18 U.S.C. 2702(a)(1), (2).

[173] 18 U.S.C. 2702(a)(3).

[174] 18 U.S.C. 2702(a)(1).

[175] 18 U.S.C. 2702(a)(2).

[176] 18 U.S.C. 2702(a)(3).

> (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
>
> (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990;
>
> (7) to a law enforcement agency – (A) if the contents – (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;
>
> (8) to a Federal, State, or local government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.[177]

The record disclosure exceptions are similar.[178]

The Ninth Circuit in *Quon* noted that the exception in paragraph 2702(b)(3)(disclosure "with the lawful consent of the originator or an addressee or intended recipient of such communication, or *the subscriber in the case of remote computing service*) permits RCS providers to disclose the contents of otherwise protected communications does not afford ECS providers the same exception.[179] Thus, the service provider violated the SCA when it supplied the Ontario Police Department (the subscriber) with the text of Sergeant Quon's pager messages.[180]

SCA: Government Access

The circumstances and procedural requirements for law enforcement access to stored wire or electronic communications and transactional records are less demanding than those under Title III.[181] They deal with two kinds of information – often in the custody of the communications service provider rather than of any of the parties to the communication – communications records and the content of electronic or wire communications. The Stored Communications Act provides two primary avenues for law enforcement access: permissible provider disclosure (section 2702) and required provided access (section 2703).[182] As noted earlier in the general discussion of

---

[177] 18 U.S.C. 2702(b)(emphasis added).

[178] "A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) – (1) as otherwise authorized in section 2703; (2) with the lawful consent of the customer or subscriber; (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency; (5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or (6) to any person other than a governmental entity," 18 U.S.C. 2702(c).

[179] *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900-903 (9th Cir. 2008), *rev'd on other grounds sub nom., City of Ontario v. Quon*, 130 S.Ct. 2619 (2010).

[180] *Id.* (ECS provider that supplied the city police department with pager service for some of its officers violated section 2702 when it provided the department with the content of the officers' pager messages).

[181] 18 U.S.C. 2701-2712.

[182] The SCA also authorizes the issuance of national security letters for foreign intelligence gathering rather than law enforcement purposes, 18 U.S.C. 2709, *see generally*, CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, by Charles Doyle.

section 2702, a public electronic communication service (ECS) provider or a public remote computing service (RCS) provider may disclose the content of a customer's communication without the consent of a communicating party to a law enforcement agency in the case of inadvertent discovery of information relating to commission of a crime,[183] or to any government entity in an emergency situation.[184] ECS and RCS providers may also disclose communications records to any governmental entity in an emergency situation.[185] Federal, state, and local agencies, regardless of the nature of their missions, all qualify as governmental entities for purposes of section 2702.[186]

Section 2702 authorizes voluntary disclosure. Section 2703 speaks to the circumstances under which ECS and RCS providers may be required to disclose communications content and related records. Section 2703 distinguishes between recent communications and those that have been in electronic storage for more than 180 days.[187] The section insists that government entities resort to a search warrant to compel providers to supply the content of wire or electronic communications held in electronic storage for less than 180 days.[188] It permits them to use a warrant, subpoena, or a court order authorized in subsection 2703(d) to force content disclosure with respect to communications held for more than 180 days.[189]

---

[183] 18 U.S.C. 2702(b)("A provider described in subsection (a) may divulge the contents of a communication . . . (7) to a law enforcement agency – (A) if the contents– (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime").

[184] 18 U.S.C. 2702(b)("A provider described in subsection (a) may divulge the contents of a communication . . . (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency").

[185] 18 U.S.C. 2702(c)("A provider described in subsection (a) may divulge the contents of a communication . . . (4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency").

[186] 18 U.S.C. 2711("As used in this chapter . . . (4) the term 'governmental entity' means a department or agency of the United States or State or political subdivision thereof"); *but see, United States v. Amawi*, 552 F.Supp.2d 679, 680 (N.D.Ohio 2008)(the Office of the Federal Public Defender is not a "governmental entity").

[187] Recall that "'electronic storage' means – (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication," 18 U.S.C. 2510(17).

[188] 18 U.S.C. 2703(a). At least one court has held that opened web-based e-mail stored on a service provider's server is no longer is "electronic storage," because the service provider storage is not necessary for backup purposes once the e-mail has been opened (i.e., after storage is not only incidental to transmission). The original remains on the web server and the service provider is simply supplying remote storage. Consequently, a governmental entity may secure access using a subpoena, *United States v. Weaver*, 636 F.Supp.2d 769, 770-72 (C.D.Ill. 2009)(distinguishing and finding unpersuasive *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), thought to support a contrary view).

[189] 18 U.S.C. 2703(a)(". . . A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section").

18 U.S.C. 2703(b)("(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection – (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity – (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title").

A subsection 2703(d) court order may be issued by a federal magistrate or by a judge qualified to issue an order under Title III.[190] It need not be issued in the district in which the provider is located.[191]

The person whose communication is disclosed is entitled to notice, unless the court authorizes delayed notification because contemporaneous notice might have an adverse impact.[192] Government supervisory officials may certify the need for delayed notification in the case of a subpoena.[193] Traditional exigent circumstances and a final general inconvenience justification form the grounds for delayed notification in either case:

- endangering the life or physical safety of an individual;
- flight from prosecution;
- destruction of or tampering with evidence;
- intimidation of potential witnesses; or
- otherwise seriously jeopardizing an investigation or unduly delaying a trial.[194]

Subsection 2703(d) authorizes issuance of an order when the governmental entity has presented specific and articulable facts sufficient to establish reasonable grounds to believe that the contents are relevant and material to an ongoing criminal investigation.[195] Some courts have held that this "reasonable grounds" standard is a *Terry* standard, a less demanding standard than "probable cause," and that under some circumstances this standard may be constitutionally insufficient to justify government access to provider held email.[196] A Sixth Circuit panel has held that the Fourth

---

[190] *Compare*, 18 U.S.C. 2703(d)("A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction. . . ."); 18 U.S.C. 2711(3)("As used in this chapter . . . (3) the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation"); 18 U.S.C. 3127(2)(emphasis added) ("As used in this chapter . . . (2) the term "court of competent jurisdiction" means – (A) any district court of the United States (*including a magistrate of such a court*) or a United States Court of Appeals having jurisdiction over the offense being investigated . . ."), *with*, 18 U.S.C. 2516(3)("Any attorney for the Government . . . may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant . . . an order authorizing or approving the interception of electronic communications . . ."); 18 U.S.C. 2510(9)(" As used in this chapter. . . 'Judge of competent jurisdiction' means – (a) a judge of a United States district court or a United States court of appeals").

[191] *United States v. Berkos,* 543 F.3d 392, 397 (7th Cir. 2008), *quoting* 18 U.S.C. 2703(a), ("[W]hen 'a court with jurisdiction over the offense' issues an out-of-district warrant for the seizure of electronic communications, it must do so 'using the procedures described in the Federal Rules of Criminal Procedure'"); *see also*, 18 U.S.C. 2711(3)(above).

[192] 18 U.S.C. 2705(a)(1)(A), (4).

[193] 18 U.S.C. 2705(a)(1)(B), (4).

[194] 18 U.S.C. 2705(a)(2), (b).

[195] 18 U.S.C. 2703(d)("A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider").

[196] *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010)(internal quotation marks and citations omitted) ("Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP. The government may not compel a commercial ISP to turn (continued...)

Amendment precludes government access to the content of stored communications (email) held by service providers in the absence of a warrant, subscriber consent, or some other indication that the subscriber has waived his or her expectation of privacy.[197] Where the government instead secures access through a subpoena or court order as section 2703 permits, the evidence may be subject to both the Fourth Amendment exclusionary rule and the exceptions to the rule.[198]

The SCA has two provisions which require providers to save customer communications at the government's request. One is found in subsection 2703(f). It requires ECS and RCS providers to preserve "records and other evidence in its possession," at the request of a governmental entity pending receipt of a warrant, court order, or subpoena.[199] Whether providers are bound to preserve emails and other communications that come into its possession both before and after receipt of the request is unclear.[200]

The second preservation provision is more detailed. It permits a governmental entity to insist that providers preserve backup copies of the communications covered by a subpoena or subsection 2703(d) court order. It gives subscribers the right to challenge the relevancy of the information sought.[201] It might also be read to require the preservation of the content of communications

(...continued)

over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional"); *see also, In re Application of the United States*, 620 F.3d 304, 313 (3d Cir. 2010)("We also conclude that this [§2703(d)] standard is a lesser one than probable cause").

[197] *United States v. Warshak*, 631 F.3d at 283-88.

[198] *Id.* at 288-92 (exception for good faith reliance on the SCA); *see also, United States v. Ferguson*, 508 F.Supp.2d 7, 8-10 D.D.C. 2007)(even if a Fourth Amendment violation occurred, officers could rely in good faith on the magistrate's order issued before any court had raised the specter of constitutional suspicion which surfaced later in *Warshak*).

[199] 18 U.S.C. 2703(f)(1)("A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process").

[200] *United States v. Warshak*, 631 F.3d 266, 283, 290 n.21 (6th Cir. 2010)(internal citations omitted)("Warshak had a number of email accounts with various ISPs, including an account with NuVox Communications. In October 2004, the government formally requested that NuVox prospectively preserve the contents of any emails to or from Warshak's email account. The request was made pursuant to 18 U.S.C. §2703(f) and it instructed NuVox to preserve all future messages. NuVox acceded to the government's request and began preserving copies of Warshak's incoming and outgoing emails – copies that would not have existed absent the prospective preservation request. Per the government's instructions, Warshak was not informed that his messages were being archived. In January 2005, the government obtained a subpoena under §2703(d) and compelled NuVox to turn over the emails that it had begun preserving the previous year. In May 2005, the government served NuVox with an *ex parte* court order under §2703(d) that required NuVox to surrender any additional email messages in Warshak's account. In all, the government compelled NuVox to reveal the contents of approximately 27,000 emails. Warshak did not receive notice of either the subpoena or the order until May 2006. . . . Some courts and commentators have suggested that §2703(f) applies only retroactively. However, the language of the statute, on its face, does not compel this reading").

[201] 18 U.S.C. 2704(b)(4)("If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed").

received by the provider both before and after receipt of the order, but the requirement that copies be made within two days of receipt of the order seems to preclude such an interpretation.[202]

Section 2703 provides greater protection to communication content than to provider records relating to those communications. Under subsection 2703(c), a governmental entity may require a ECS or RCS provider to disclose records or information pertaining to a customer or subscriber – other than the content of a communication – under a warrant, a court order under subsection 2703(d), or with the consent of the subject of the information.[203] An administrative, grand jury or trial subpoena is sufficient, however, for a limited range of customer or subscriber related information.[204] The customer or subscriber need not be notified of the record disclosure in either case.[205]

The district courts have been divided for some time over the question of what standard applies when the government seeks cell phone location information from a provider, either current or historical.[206] The Third Circuit has held that while issuance of an order under subsection 2703(d) does not require a showing of probable cause as a general rule, the circumstances of a given case may require it.[207]

SCA: Consequences

Breaches of the unauthorized access prohibitions of section 2701 expose offenders to possible criminal, civil, and administrative sanctions. Violations committed for malicious, mercenary, tortious or criminal purposes are punishable by imprisonment for not more than five years (not more than 10 years for a subsequent conviction) and/or a fine of not more than $250,000 (not more than $500,000 for organizations); lesser transgressions, by imprisonment for not more than one year (not more than five years for a subsequent conviction) and/or a fine of not more than

---

[202] 18 U.S.C. 2704(a)(1), (2)(emphasis added)("A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. *Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.* (2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a)").

[203] 18 U.S.C. 2703(c)(1).

[204] 18 U.S.C. 2703(c)(2)("A provider of electronic communication service or remote computing service shall disclose to a governmental entity the (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment (including any credit car or bank account number), of a subscriber to or customer of such service, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1)"); *United States v. Cray*, 673 F.Supp.2d 1368, 1378-379 (S.D.Ga. 2009).

[205] 18 U.S.C. 2703(c)(3).

[206] *See, In re Application of the United States*, 733 F.Supp.2d 939, 940 n.1 (N.D.Ill. 2009)(listed cases decided up to that point).

[207] *In re Application of the United States*, 620 F.3d 304, 313-19 (3d Cir. 2010); *see also*, *In re Application of the United States*, ___ F.Supp.2d ___, ___ (S.D.Tex. Oct. 29, 2010)(access to provider records relating to cell phone location over the course of an earlier two month period requires a warrant); *In re Application of the United States*, 727 F.Supp.2d 571, 583-84 (W.D.Tex. 2010)(access to provider records relating to cell phone location either historically or prospectively should be only be available under a warrant, at least until a circuit court rules otherwise).

$100,000.[208] Victims of a violation of subsection 2701(a) have a cause of action for equitable relief, reasonable attorneys' fees and costs, damages equal the loss and gain associated with the offense but not less than $1,000.[209]

Violations by the United States may give rise to a cause of action and may result in disciplinary action against offending officials or employees under the same provisions that apply to U.S. violations of Title III,[210] Unlike violations of Title III, however, there is no statutory prohibition on disclosure or use of the information through a violation of section 2701;[211] nor is there a statutory rule for the exclusion of evidence as a consequence of a violation.[212] Yet, violations of SCA, which also constitute violations of the Fourth Amendment, will trigger both the Fourth Amendment exclusionary rule and the exceptions to that rule.[213]

No criminal penalties attend a violation of voluntary provider disclosure prohibitions of section 2702. Yet, ECS and RCS providers – unable to claim the benefit of one of the section's exceptions, of the good faith defense under subsection 2707(e), or of the immunity available under subsection 2703(e) – may be liable for civil damages, costs and attorneys' fees under section 2707 for any violation of section 2702.[214]

---

[208] "The punishment for an offense under subsection (a) of this section is – (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the constitution and laws of the United States or any state – (A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and (B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and (2)(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section,"18 U.S.C. 2701(b).

[209] "(a) Cause of action – Except as provided in section 2703(e)[relating to immunity for compliance with judicial process], any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity other than the United States which engaged in that violation such relief as may be appropriate.

"(b) Relief – In a civil action under this section, appropriate relief includes – (1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection(c); and (3) a reasonable attorney's fee and other litigation costs reasonably incurred;

"(c) Damages – The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. . . ." 18 U.S.C. 2707.

To be eligible for statutory damages, a plaintiff must show actual damage, but attorneys' fees and punitive damages may be award without proof of actual damages, *VanAlystyne v. Electronic Scriptorium, Ltd.*, 560 F.3d 199, 202 (4th Cir. 2009).

[210] "Any person who is aggrieved by any willful violation this chapter or of chapter 119 of this title [18 U.S.C. 2510-2520] . . . may commence an action in United States District Court . . . .If . . . any of the departments or agencies has violated any provision of this chapter . . . the department or agency shall . . . promptly initiate a proceeding to determine whether disciplinary action . . . is warranted. . . ."18 U.S.C. 2712(a),(c).

[211] *Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 976 (M.D.Tenn. 2008).

[212] *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008); *United States v. Clenney*, 631 F.3d 658, 667 (11th Cir. 2011); *United States v. Navas*, 640 F.Supp.2d 256, 262 (S.D.N.Y. 2009).

[213] *See e.g., United States v. Warshak*, 631 F.3d 266, 282-89 (6th Cir. 2010).

[214] No liability under section 2707 accrues, however, as a consequence of aiding or abetting a provider's violation of section 2702, *Freeman v. DirecTV*, 457 F.3d 1001, 1009 (9th Cir. 2006).

Pen Registers and Trap and Trace Devices (PR/T&T)

PR/T&T: Prohibitions

A trap and trace device identifies the source of incoming calls, and a pen register indicates the numbers called from a particular instrument.[215] Since they did not allowed the user to overhear the "contents" of the phone conversation or to otherwise capture the content of a communication, they were not considered interceptions within the reach of Title III prior to the enactment of ECPA.[216] Although Congress elected to expand the definition of interception, it chose to regulate these devices beyond the boundaries of Title III for most purposes.[217] Nevertheless, the Title III wiretap provisions apply when, due to the nature of advances in telecommunications technology, pen registers and trap and trace devices are able to capture wire communication "content."[218]

The USA PATRIOT Act enlarged the coverage of sections 3121-3127 to include sender/addressee information relating to email and other forms of electronic communications.[219]

Subsection 3121(a) outlaws installation or use of a pen register or trap and trace device, except under one of seven circumstances:

- pursuant to a court order issued under sections 3121-3127;
- pursuant to a Foreign Intelligence Surveillance Act (FISA) court order;[220]
- with the consent of the user;
- when incidental to service;

---

[215] "(3) [T]he term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; (4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted," 18 U.S.C. 3127(3),(4). Although clone pagers are not considered pen registers, *Brown v. Waddell*, 50 F.3d 285, 290-91 (4th Cir. 1995), "caller id" services have been found to constitute trap and trace devices by some courts, *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995), but not others, *Sparshott v. Feld Entertainment, Inc.*, 311 F.3d 425, 432-33 (D.C.Cir. 2003).

[216] *United States v. New York Telephone Co.*, 434 U.S. 159 (1977).

[217] 18 U.S.C. 3121 – 3127.

[218] "'Post-cut-through dialed digits' are any numbers dialed from a telephone after the call is initially setup or 'cut-through.' Sometimes these digits are other telephone numbers, as when a party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party. Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like. In the latter case, the digits represent communications content; in the former, they are non-content call processing numbers," *In re United States*, 441 F.Supp.2d 816, 818 (S.D. Tex. 2006); *see also*, *In re United States for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices*, 515 F.Supp.2d 325, 328-38 (E.D.N.Y. 2007); *In re United States*, 622 F.Supp.2d 411, 419-22 (S.D. Tex. 2007).

[219] 115 Stat. 288-91 (2001).

[220] 18 U.S.C. 3121 ("Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)").

- when necessary to protect users from abuse of service;
- when necessary to protect providers from abuse of service;[221] or
- in an emergency situation.[222]

PR/T&T: Government Access

Federal government attorneys and state and local police officers may apply for a court order authorizing the installation and use of a pen register and/or a trap and trace device upon certification that the information that it will provide is relevant to a pending criminal investigation.[223]

An order authorizing installation and use of a pen register or trap and trace device must:

- specify
    - the person (if known) upon whose telephone line the device is to be installed,
    - the person (if known) who is the subject of the criminal investigation,
    - the telephone number, (if known) the location of the line to which the device is to be attached, and geographical range of the device,
    - a description of the crime to which the investigation relates;
- upon request, direct carrier assistance pursuant to section 3124;
- terminate within 60 days, unless extended;
- involve a report of particulars of the order's execution in Internet cases; and

[221] 18 U.S.C. 3121(b)("The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service – (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained").

[222] 18 U.S.C. 3125(a)("Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that — (1) an emergency situation exists that involves – A) immediate danger of death or serious bodily injury to any person; (B) conspiratorial activities characteristic of organized crime; (C) an immediate threat to a national security interest; or (D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year [–] that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and (2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use [—] may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title").

[223] 18 U.S.C. 3122.

- impose necessary nondisclosure requirements.[224]

The order may be issued by a judge of "competent jurisdiction" over the offense under investigation, including a federal magistrate judge.[225] Senior Justice Department or state prosecutors may approve the installation and use of a pen register or trap and trace device prior to the issuance of court authorization in emergency cases that involve either an organized crime conspiracy, an immediate danger of death or serious injury, a threat to national security, or a serious attack on a "protected computer."[226] Emergency use must end within 48 hours, or sooner if an application for court approval is denied.[227]

Federal authorities have applied for court orders, under the Stored Communications Act (18 U.S.C. 2701-2712) and the trap and trace authority of 18 U.S.C. 3121-3127, seeking to direct communications providers to supply them with the information necessary to track cell phone users in conjunction with an ongoing criminal investigation. Thus far, their efforts have met with mixed success.[228]

PRT&T: Consequences

The use or installation of pen registers or trap and trace devices by anyone other than the telephone company, service provider, or those acting under judicial authority is a federal crime, punishable by imprisonment for not more than a year and/or a fine of not more than $100,000 ($200,000 for an organization).[229] Subsection 3124(e) creates a good faith defense for reliance upon a court order under subsection 3123(b), an emergency request under subsection 3125(a), "a legislative authorization, or a statutory authorization."[230] There is no accompanying exclusionary rule, and consequently a violation of section 3121 will not serve as a basis to suppress any resulting evidence.[231]

Moreover, unlike violations of Title III, there is no requirement that the target of an order be notified upon the expiration of the order nor a separate federal private cause of action for victims of a pen register or trap and trace device violation.[232] Some of the states have established a

---

[224] 18 U.S.C. 3123.

[225] 18 U.S.C. 3122(a), 3127(2); *In re United States*, 10 F.3d 931, 935-36 (2d Cir. 1993).

[226] 18 U.S.C. 3125(a).

[227] 18 U.S.C. 3121(b).

[228] *E.g., In re Application of the United States*, 534 F.Supp.2d 585 (W.D.Pa. 2008); In *re Application of the United States*, 497 F.Supp.2d 301 (D. P.R. 2007); *In re United States*, 441 F.Supp.2d 816 (S.D. Tex. 2006); *In re Application of the United States*, 416 F.Supp. 390 (D.Md. 2006); *In re Application of the United States*, 415 F.Supp.2d 211 (W.D.N.Y. 2006); *In re Application of the United States*, 412 F.Supp.2d 947 (E.D.Wis. 2006); *In re Application of the United States*, 407 F.Supp.2d 134 (D.D.C. 2006) (each denying the application); *but see*, *In re Application of the United States*, 632 F.Supp.2d 202 (E.D.N.Y. 2008); *In re Application of the United States*, 509 F.Supp.2d 76 (D.Mass. 2007); *In re Application of the United States*, 460 F.Supp.2d 448 (S.D.N.Y. 2006); *In re Application of the United States*, 433 F.Supp.2d 804 (S.D. Tex. 2006); *In re Application of the United States*, 411 F.Supp.2d 678 (W.D.La. 2006).

[229] 18 U.S.C. 3121(d), 3571.

[230] 18 U.S.C. 3124(e).

[231] *United States v. Forrester*, 512 F.3d 500, 512-13 (9th Cir. 2008); *United States v. German*, 486 F.3d 849, 852-53 (5th Cir. 2007); *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995); *United States v. Thompson*, 936 F.2d 1249, 1249-250 (11th Cir. 1991). To the extent that the unlawful use captures content, the Fourth Amendment exclusionary rule may apply, *cf., In re United States for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices*, 515 F.Supp.2d 325, 328-38 (E.D.N.Y. 2007).

[232] Subsection 3124(d) makes the denial of a cause of action explicit for service providers and others assisting in (continued...)

separate criminal offense for unlawful use of a pen register or trap and trace device,[233] yet most of these seem to follow the federal lead and decline to establish a separate private cause of action for unlawful installation or use of the devices.[234]

(...continued)

exeuction of an order or emergency request. Subsection 3124(e) provides a good faith defense to civil liability on other grounds.

[233] *E.g.*, ARIZ. REV. STAT. ANN. §13-3005; FLA. STAT. ANN. §934.31; IOWA CODE ANN. §808B.10; N.H. RV. STAT. ANN. §570-B:2; UTAH CODE ANN. §77-23-13.

[234] *But see*, MINN. STAT. ANN. §626A.391. Appendix E contains the citations of state statutes that authorized court ordered installation and use of pen registers and trap & trace devices. Appendix C lists the citations of state statutes that create a separate cause of action for unlawful interception.

Appendix A. State Statutes Outlawing the Interception of Wire(w), Oral(o) and Electronic Communications(e)

Alabama: Ala.Code §§13A-11-30 to 13A-11-37(w/o);
Alaska: Alaska Stat. §§42.20.300 to 42.20.390 (w/o/e);
Arizona: Ariz.Rev.Stat.Ann. §§13-3001 to 13-3009 (w/o/e);
Arkansas: Ark.Code §§5-60-120, 23-17-107(w/o/e);
California: Cal.Penal Code §§631(w), 632(o), 632.7(e);
Colorado: Colo.Rev.Stat. §§18-9-301 to 18-9-305(w/o/e);

Connecticut: Conn.Gen.Stat.Ann. §§53a-187 to 53a-189, 54-41t (w/o);
Delaware: Del.Code tit.11 §§ 2401, 2402(w/o/e);
Florida: Fla.Stat.Ann. §§ 934.02, 934.03(w/o/e);
Georgia: Ga.Code §16-11-62 (w/o/e);
Hawaii: Hawaii Rev.Stat. §§ 711-1111, 803-41, 803-42(w/o/e);
Idaho: Idaho Code §§ 18-6701, 18-6702(w/o/e);

Indiana: Ind.Code Ann. §§ 35-33.5-1-5, 35-33.5-5-5(w/e);
Iowa: Iowa Code Ann. §§272.8, 808B.2(w/o/e);
Kansas: Kan.Stat.Ann. §21-4001(w/o); 21-4002(w);
Kentucky: Ky.Rev.Stat. §§526.010, 526.020(w/o);
Louisiana: La.Rev.Stat.Ann. §§ 15:1302, 15:1303 (w/o/e);
Maine: Me.Rev.Stat.Ann. tit. 15 §§ 709, 710(w/o);

Maryland: Md.Cts. & Jud.Pro.Code Ann. §§ 10-401, 10-402(w/o/e);
Massachusetts: Mass.Gen.Laws Ann. ch.272 §99 (w/o);
Michigan: Mich.Comp.Laws Ann. §§750.539a, 750.539c(o); 750.540(w);
Minnesota: Minn.Stat.Ann. §§ 626A.01, 626A.02 (w/o/e);

Mississippi: Miss.Code §41-29-533(w/o/e)
Missouri: Mo.Ann.Stat. §§ 542.400 to 542.402 (w/o);
Montana: Mont.Code Ann. §45-8-213(w/o/e);
Nebraska: Neb.Rev.Stat. §§ 86-271 to 86-290 (w/o/e);
Nevada: Nev.Rev.Stat. §§ 200.610, 200.620(w), 200.650(o);
New Hampshire: N.H.Rev.Stat.Ann. §§ 570-A:1, 570-A:2 (w/o);

New Jersey: N.J.Stat.Ann. §§ 2A:156A-2, 2A:156A-3(w/o/e);
New Mexico: N.M.Stat.Ann. §30-12-1(w);
New York: N.Y.Penal Law §§ 250.00, 250.05(w/o/e);
North Carolina: N.C.Gen.Stat. §§ 15A-286, 15A-287(w/o/e);
New Hampshire: N.H.Rev.Stat.Ann. §§ 570-A:1, 570-A:2 (w/o);

New Jersey: N.J.Stat.Ann. §§ 2A:156A-2, 2A:156A-3(w/o/e);
New Mexico: N.M.Stat.Ann. §30-12-1(w);
New York: N.Y.Penal Law §§ 250.00, 250.05(w/o/e);
North Carolina: N.C.Gen.Stat. §§ 15A-286, 15A-287(w/o/e);
North Dakota: N.D.Cent.Code §§12.1-15-02, 12.1-15-04 (w/o);

Ohio: Ohio Rev.Code §§ 2933.51, 2933.52 (w/o/e);
Oklahoma: Okla.Stat.Ann. tit.13 §§ 176.2, 176.3 (w/o/e);
Oregon: Ore.Rev.Stat. §§165.535 to 165.545 (w/o/e);
Pennsylvania: Pa.Stat.Ann. tit.18 §§ 5702, 5703 (w/o/e);
Rhode Island: R.I.Gen.Laws §§11-35-21(w/o/e);
South Carolina: S.C. Code Ann. §§16-17-470, 17-30-10 to 17-30-20 (w/o/e);

South Dakota: S.D.Cod.Laws §§ 23A-35A-1, 23A-35A-20 (w/o);
Tennessee: Tenn.Code Ann. §39-13-601(w/o/e);
Texas: Tex.Penal Code. § 16.02; Tex. Crim. Pro. Code art. 18.20 (w/o/e);
Utah: Utah Code Ann. §§ 76-9-405, 77-23a-3, 77-23a-4 (w/o/e);

Virginia: Va.Code §§ 19.2-61, 19.2-62(w/o/e);
Washington: Wash.Rev.Code Ann.§9.73.030 (w/o);
West Virginia: W.Va.Code §§ 62-1D-2, 62-1D-3(w/o/e);
Wisconsin: Wis.Stat.Ann. §§ 968.27, 968.31(w/o/e);
Wyoming: Wyo.Stat. §§ 7-3-701, 7-3-702(w/o/e);
District of Columbia: D.C.Code §§ 23-541, 23-542(w/o).

Appendix B. Consent Interceptions Under State Law

Alabama: Ala.Code §13A-11-30 (one party consent);
Alaska: Alaska Stat. §§42.20.310, 42.20.330 (one party consent);
Arizona: Ariz.Rev.Stat.Ann. §13-3005 (one party consent);
Arkansas: Ark.Code §5-60-120 (one party consent);
California: Cal. Penal Code §§ 631, 632 (one party consent for police; all party consent otherwise), 632.7 (all party consent);

Colorado: Colo.Rev.Stat. §§18-9-303, 18-9-304 (one party consent);
Connecticut: Conn.Gen.Stat.Ann. §§53a-187, 53a-188 (criminal proscription: one party consent); §52-570d (civil liability: all party consent except for police);
Delaware: Del.Code tit.11 §2402 (one party consent);
Florida: Fla.Stat.Ann. §934.03 (one party consent for the police; all party consent for others);

Georgia: Ga.Code §16-11-66 (one party consent);
Hawaii: Hawaii Rev.Stat. §§ 711-1111, 803-42 (one party consent);
Idaho: Idaho Code §18-6702 (one party consent);
Illinois: Ill.Comp.Stat.Ann. ch.720 §§5/14-2, 5/14-3 (all party consent with law enforcement exceptions);
Indiana: Ind.Code Ann. §35-33.5-1-5 (one party consent);
Iowa: Iowa Code Ann. §808B.2 (one party consent);

Kansas: Kan.Stat.Ann. §§21-4001, 21-4002 (one party consent);
Kentucky: Ky.Rev.Stat. §526.010 (one party consent);
Louisiana: La.Rev.Stat.Ann. §15:1303 (one party consent);
Maine: Me.Rev.Stat.Ann. tit. 15 §709 (one party consent);
Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-402 (all party consent);
Massachusetts: Mass.Gen.Laws Ann. ch.272 §99 (all parties must consent, except in some law enforcement cases);

Michigan: Mich.Comp.Laws Ann. §750.539c (proscription regarding eavesdropping on oral conversation: all party consent, except that the proscription does not apply to otherwise lawful activities of police officers);
Minnesota: Minn.Stat.Ann. §626A.02 (one party consent);
Mississippi: Miss.Code §41-29-531 (one party consent);
Missouri: Mo.Ann.Stat. §542.402 (one party consent);

Montana: Mont.Code Ann. §§45-8-213 (all party consent with an exception for the performance of official duties);
Nebraska: Neb.Rev.Stat. § 86-290 (one party consent);
Nevada: Nev.Rev.Stat. §§200.620, 200.650 (one party consent);
New Hampshire: N.H.Rev.Stat.Ann. §570-A:2 (all party consent);
New Jersey: N.J.Stat.Ann. §§2A:156A-4 (one party consent);

New Mexico: N.M.Stat.Ann. §§30-12-1 (one party consent);
New York: N.Y.Penal Law §250.00 (one party consent);
North Carolina: N.C.Gen.Stat. §15A-287 (one party consent);
North Dakota: N.D.Cent.Code §§12.1-15-02 (one party consent);
Ohio: Ohio Rev.Code §2933.52 (one party consent);

Oklahoma: Okla.Stat.Ann. tit.13 §176.4 (one party consent);
Oregon: Ore.Rev.Stat. §165.540 (one party consent for wiretapping and all parties must consent for other forms of electronic eavesdropping);
Pennsylvania: Pa.Stat.Ann. tit.18 §5704 (one party consent for the police; all parties consent otherwise);
Rhode Island: R.I.Gen.Laws §§11-35-21 (one party consent);

South Carolina: S.C. Code Ann. § 17-30-30 (one party consent);
South Dakota: S.D.Comp.Laws §§23A-35A-20 (one party consent);
Tennessee: Tenn.Code Ann. §39-13-601 (one party consent)
Texas: Tex.Penal Code §16.02 (one party consent);
Utah: Utah Code Ann. §§77-23a-4 (one party consent);
Virginia: Va.Code §19.2-62 (one party consent);

Washington: Wash.Rev.Code Ann. §9.73.030 (all parties must consent, except that one party consent is sufficient in certain law enforcement cases);
West Virginia: W.Va.Code §62-1D-3 (one party consent);
Wisconsin: Wis.Stat.Ann. §968.31 (one party consent);
Wyoming: Wyo.Stat. §7-3-702 (one party consent);
District of Columbia: D.C.Code §23-542 (one party consent).

Appendix C. Statutory Civil Liability for Interceptions Under State Law

Arizona: Ariz.Rev.Stat.Ann. §12-731;
California: Cal. Penal Code §§ 637.2;
Colorado: Colo.Rev.Stat. §18-9-309.5;
Connecticut: Conn.Gen.Stat.Ann. §§54-41r, 52-570d;
Delaware: Del.Code tit.11 §2409;

Florida: Fla.Stat.Ann. §§934.10, 934.27;
Hawaii: Hawaii Rev.Stat. §803-48;
Idaho: Idaho Code §18-6709;
Illinois: Ill.Comp.Stat.Ann. ch.720 §5/14-6;
Indiana: Ind.Code Ann. §35-33.5-5-4;

Iowa: Iowa Code Ann. §808B.8;
Kansas: Kan.Stat.Ann. §22-2518
Louisiana: La.Rev.Stat.Ann. §15:1312;
Maine: Me.Rev.Stat.Ann. ch.15 §711;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-410, 10-4A-08;

Massachusetts: Mass.Gen.Laws Ann. ch.272 §99;
Michigan: Mich.Comp.Laws Ann. §750.539h;
Mississippi: Miss. Code § 41-29-529;
Minnesota: Minn.Stat.Ann. §§626A.02, 626A.13;
Nebraska: Neb.Rev.Stat. § 86-297;

Nevada: Nev.Rev.Stat. §200.690;
New Hampshire: N.H.Rev.Stat.Ann. §570-A:11;
New Jersey: N.J.Stat.Ann. §§2A:156A-24;
New Mexico: N.M.Stat.Ann. §§30-12-11;
North Carolina: N.C.Gen.Stat. §15A-296;

Ohio: Ohio Rev.Code §2933.65;
Oregon: Ore.Rev.Stat. §133.739;
Pennsylvania: Pa.Stat.Ann. tit.18 §§5725, 5747;
Rhode Island: R.I.Gen.Laws §12-5.1-13;
South Carolina: S.C. Code Ann. § 17-30-135;

Tennessee: Tenn.Code Ann. §39-13-603;
Texas: Tex.Code Crim.Pro. art. 18.20;
Utah: Utah Code Ann. §§77-23a-11; 77-23b-8;
Virginia: Va.Code §19.2-69;
Washington: Wash.Rev.Code Ann. §9.73.060;

West Virginia: W.Va.Code §62-1D-12;
Wisconsin: Wis.Stat.Ann. §968.31;
Wyoming: Wyo.Stat. §7-3-710;
District of Columbia: D.C.Code §23-554.

Appendix D. Court Authorized Interception Under State Law

Alaska: Alaska Stats. §§12.37.010 to 12.37.900;
Arizona: Ariz.Rev.Stat.Ann. §§13-3010 to 13-3019;
California: Cal.Penal Code §629.50 to 629.98;
Colorado: Colo.Rev.Stat. §§16-15-101 to 16-15-104;
Connecticut: Conn.Gen.Stat.Ann. §§54-41a to 54-41u;

Delaware: Del.Code tit.11 §§2401 to 2412;
Florida: Fla.Stat.Ann. §§934.02 to 934.43;
Georgia: Ga.Code §16-11-64 to 16-11-69;
Hawaii: Hawaii Rev.Stat. §§803-41 to 803-49;
Idaho: Idaho Code §§18-6701 to 18-6709; 6719 to 6725;

Illinois: Ill.Stat.Ann. ch.725 §§5/108A-1 to 108B-14;
Indiana:Ind.Code §§35-33.5-1-1 to 35-33.5-5-6;
Iowa: Iowa Code Ann. §§808B.3 to 808B.7;
Kansas: Kan.Stat.Ann. §§ 22-2514 to 22-2519;
Louisiana: La.Rev.Stat.Ann. §§15:1301 to 15:1316;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-401 to 10-410;

Massachusetts: Mass.Gen.Laws Ann. ch.272 §99;
Minnesota: Minn.Stat.Ann. §§626A.01 to 626.41;
Mississippi: Miss.Code §§41-29-501 to 41-29-537;
Missouri: Mo.Ann.Stat. §§542.400 to 542.422;
Nebraska: Neb.Rev.Stat. §§ 86-271 to 86-2,115;

Nevada: Nev.Rev.Stat. §§179.410 to 179.515;
New Hampshire: N.H.Rev.Stat.Ann. §§570-A:1 to 570-A:9;
New Jersey: N.J.Stat.Ann. §§2A:156A-8 to 2A:156A-26;
New Mexico: N.M.Stat.Ann. §§30-12-1 to 30-12-11;
New York: N.Y.Crim.Pro. Law §§700.05 to 700.70;

North Carolina: N.C.Gen.Stat. §§15A-286 to 15A-298;
North Dakota: N.D.Cent.Code §§29-29.2-01 to 29-29.2-05;
Ohio: Ohio Rev.Code §§2933.51 to 2933.66;
Oklahoma: Okla.Stat.Ann. tit.13 §§176.1 to 176.14
Oregon: Ore.Rev.Stat. §§133.721 to 133.739;

Pennsylvania: Pa.Stat.Ann. tit.18 §§5701 to 5728
Rhode Island: R.I.Gen.Laws §§12-5.1-1 to 12-5.1-16;
South Carolina: S.C. Code Ann. §§ 17-30-10 to 17-30-145;

South Dakota: S.D.Cod.Laws §§23A-35A-1 to 23A-35A-34;
Tennessee: Tenn.Code Ann. §§40-6-301 to 40-6-311;
Texas: Tex.Crim.Pro. Code. art. 18.20;
Utah: Utah Code Ann. §§77-23a-1 to 77-23a-16;
Virginia: Va.Code §§19.2-61 to 19.2-70.3;

Washington: Wash.Rev.Code Ann. §§9.73.040 to 9.73.250;
West Virginia: W.Va.Code §§62-1D-1 to 62-1D-16;
Wisconsin: Wis.Stat.Ann. §§968.27 to 968.33;
Wyoming: Wyo.Stat. §§7-3-701 to 7-3-712;
District of Columbia: D.C.Code §§23-541 to 23-556.

Appendix E. State Statutes Regulating Stored Electronic Communications (SE), Pen Registers (PR) and Trap and Trace Devices (T)

Alaska: Alaska Stats. §§12.37.200 (PR&T), 12.37.300(SE);
Arizona: Ariz.Rev.Stat.Ann. §§13-3016 (SE); 13-3005, 13-3017 (PR&T);
Arkansas: Ark. Code Ann. § 5-60-120(g) (PR&T);
Colorado: Colo. Rev. Stat. § 18-9-305 (PR&T);
Delaware: Del.Code tit.11 §§ 2401; 2421 to 2427 (SE); 2430 to 2434 (PR&T);

Florida: Fla.Stat.Ann. §§934.02; 934.21 to 934.28 (SE); 934.32 to 934.34(PR&T);
Georgia: Ga.Code Ann. §§16-11-60 to 16-11-64.2 (PR &T); § 16-9-109 (SE);
Hawaii: Hawaii Rev.Stat. §§803-41; 803-44.5, 803-44.6 (PR&T), 803-47.5 to 803.47.9 (SE);
Idaho: Idaho Code §§18-6719 to 18-6725 (PR&T);
Iowa: Iowa Code Ann. §§808B.1, 808B.10 to 808B.14 (PR&T);

Kansas: Kan.Stat.Ann. §§22-2525 to 22-2529 (PR&T);
Louisiana: La.Rev.Stat.Ann. §§15:1302, 15:1313 to 15:1316 (PR&T);
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-4A-01 to 10-4A-08 (SE), 10-4B-01 to 10-4B-05 (PR&T);
Minnesota: Minn.Stat.Ann. §§626A.01; 626A.26 to 626A.34; (SE), 626A.35 to 636A.391 (PR&T);
Mississippi: Miss.Code §41-29-701(PR&T);

Missouri: Mo.Ann.Stat. §542.408 (PR);
Montana: Mont.Code Ann. §§46-4-401 to 46-4-405 (PR&T);
Nebraska: Neb.Rev.Stat. §§ 86-279, 86-2,104 to 86-2,110 (SE); 86-284, 86-287, 86-298 to 86-2,101 (PR&T);
Nevada: Nev.Rev.Stat. §§179.530 (PR&T), 205.492 to 205.513(SE);
New Hampshire: N.H.Rev.Stat.Ann. §§570-B:1 to 570-B:7 (PR&T);
New Jersey; N.J.Stat.Ann. §§2A:156A-27 to 2A:156A-34 (SE);
New York: N.Y.Crim.Pro.Law §§705.00 to 705.35 (PR&T);
North Carolina: N.C.Gen.Stat. §§15A-260 to 15A-264 (PR&T);
North Dakota: N.D.Cent.Code §§29-29.3-01 to 29-29.3-05 (PR&T);

Ohio: Ohio Rev.Code §2933.76 (PR&T);
Oklahoma: Okla.Stat.Ann. tit.13 §177.1 to 177.5 (PR&T);
Oregon: Ore.Rev.Stat. §§165.657 to 165.673 (PR&T);
Pennsylvania: Pa.Stat.Ann. tit.18 §§5741 to 5749 (SE), 5771 to 5775 (PR&T);
Rhode Island; R.I.Gen.Laws §§12-5.2-1 to 12-5.2-5 (PR&T);

South Carolina: S.C.Code §§17-29-10 to 17-29-50, 17-30-45 to 17-30-50 (PR&T);
South Dakota: S.D.Cod.Laws §§23A-35A-22 to 23A-35A-34 (PR&T);
Tennessee: Tenn.Code Ann. §40-6-311 (PR&T);
Texas: Tex.Code Crim.Pro. art. 18.20, 18.21; Tex. Penal Code §§ 16.03, 16.04 (SE, PR&T);
Utah: Utah Code Ann. §§77-23a-13 to 77-23a-15 (PR&T); 77-23b-1 to 77-23b-9(SE);

Virginia: Va.Code §§19.2-70.1, 19.2-70.2 (PR&T), 19.2-70.3 (SE);
Washington: Wash.Rev.Code Ann. §9.73.260 (PR&T);
West Virginia: W.Va.Code §§62-1D-2, 62-1D-10 (PR&T);
Wisconsin: Wis.Stat.Ann. §968.30 to 968.37 (PR&T);
Wyoming: Wyo.Stat. §§7-3-801 to 7-3-806 (PR&T).

Appendix F. State Computer Crime Statutes

Alabama: Ala.Code §§13A-8-100 to 13A-8-103;
Alaska: Alaska Stat. §11.46.740;
Arizona: Ariz.Rev.Stat.Ann. §§13-2316 to 13-2316.02;
Arkansas: Ark.Code §§5-41-101 to 5-41-206;
California: Cal.Penal Code §502;

Colorado: Colo.Rev.Stat. §§18-5.5-101, 18-5.5-102;
Connecticut: Conn.Gen.Stat.Ann. §§53a-250 to 53a-261;
Delaware: Del.Code tit.11 §§931 to 941;
Florida: Fla.Stat.Ann. §§815.01 to 815.07;
Georgia: Ga.Code §§16-9-92 to 16-9-94;

Hawaii: Hawaii Rev.Stat. §708-890 to 708-895.7;
Idaho: Idaho Code §§18-2201, 18-2202;
Illinois: Ill.Stat.Ann. ch.720 §§5/16D-1 to 5/16D-7;
Indiana: Ind.Code §§35-43-1-4 to 35-43-2-3;
Iowa: Iowa Code Ann. §716.6B;

Kansas: Kan.Stat.Ann. §21-3755;
Kentucky: Ky.Rev.Stat. §§434.840 to 434.860;
Louisiana: La.Rev.Stat.Ann. §§14:73.1 to 14:73.7;
Maine: Me.Rev.Stat.Ann. tit. 17-A §§431 to 433;
Maryland: Md.Code Ann., Crim. Law. §7-302;
Massachusetts: Mass.Gen.Laws Ann. ch.266 §120F;

Michigan: Mich.Comp.Laws Ann. §§752.791 to 752.797;
Minnesota: Minn.Stat.Ann. §§609.87 to 609.893;
Mississippi: Miss.Code §§97-45-1 to 97-45-29;
Missouri: Mo.Ann.Stat. §§569.095 to 569.099;
Montana: Mont.Code Ann. §§45-6-310, 45-6-311;
Nebraska: Neb.Rev.Stat. §§28-1341 to 28-1348;

Nevada: Nev.Rev.Stat. §§205.473 to 205.492; 205.509 to 205.513;
New Hampshire: N.H.Rev.Stat.Ann. §638:16 to 638:19;
New Jersey: N.J.Stat.Ann. §§2C:20-2, 2C:20-23 to 2C:20-34;

New Mexico: N.M.Stat.Ann. §§30-45-1 to 30-45-7;
New York: N.Y.Penal Law §§156.00 to 156.50;
North Carolina: N.C.Gen.Stat. §§14-453 to 14-458;
North Dakota: N.D.Cent.Code §12.1-06.1-08;
Ohio: Ohio Rev.Code §§2909.01, 2909.07, 2913.01 to 2913.04, 2913.421;

Oklahoma: Okla.Stat.Ann. tit.21 §§1951 to 1959;
Oregon: Ore.Rev.Stat. §164.377;
Pennsylvania: Pa.Stat.Ann. tit.18 §7611;
Rhode Island: R.I.Gen.Laws §§11-52-1 to 11-52-8;
South Carolina: S.C.Code §§16-16-10 to 16-16-40, 26-6-210;

South Dakota: S.D.Cod.Laws §§43-43B-1 to 43-43B-8;
Tennessee: Tenn.Code Ann. §§39-14-601 to 39-14-605;
Texas: Tex.Penal Code. §§33.01 to 33.05;
Utah: Utah Code Ann. §§76-6-702 to 76-6-705;

Vermont: Vt. Stat. Ann. tit. 13, §§ 4101 to 4107;
Virginia: Va.Code §§18.2-152.1 to 18.2-152.15, 19.2-249.2;
Washington: Wash.Rev.Code Ann. §§9A.52.110 to 9A.52.130;
West Virginia: W.Va.Code §§61-3C-1 to 61-3C-21;
Wisconsin: Wis.Stat.Ann. §943.70;
Wyoming: Wyo.Stat. §§6-3-501 to 6-3-505.

Appendix G. Spyware[235]

Alaska: Alaska Stat. §§ 45.45.471 to 45.45.798;

Arizona: Ariz. Rev. Stat. Ann. §§ 44-7301 to 44-7304**;**

Arkansas: Ark. Code §§ 4-110-101 to 4-110-105;

California: Cal. Bus. & Prof. Code §§ 22947 to 22947.6;

Georgia: Ga. Code Ann. §§ 16-9-150 to 16-9-157;

Indiana: Ind. Code Ann. §§ 24-4.8-1-1 to 24-4.8-3-2;

Iowa: Iowa Code Ann. §§ 714F.1 to 714F.8;

Louisiana: La. Rev. Stat. Ann. §§ 51:2006 to 51:2014;

Nevada: Nev. Rev. Stat. Ann. §205.4737;

New Hampshire: N.H. Rev. Stat. Ann. §§ 359-H:1 to 359-H:6;

Texas: Tex. Bus. & Com. Code Ann. §§ 48.001 to 48.102;

Utah: Utah Code Ann. §§ 13-40-101 to 13-40-401;

Washington: Wash. Rev. Code Ann. §§19.270.010 to 19.270.900.

[235] Depending upon the definition used, spyware has been outlawed under a host of federal and state laws; this appendix is limited to those state statutes that address "spyware" as such. For a general discussion of activities at the federal level *see*, CRS Report RL32706, *Spyware: Background and Policy Issues for Congress*.

Appendix H. Text of Electronic Communications Privacy Act (ECPA)

18 U.S.C. 2510. Definitions.

As used in this chapter–

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than–

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b)a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) "Investigative or law enforcement officer" means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) "Judge of competent jurisdiction" means –

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) "communication common carrier" has the meaning given the term in section 3 of the Communications Act of 1934;

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include–

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who–

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not–

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means–

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means –

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against –

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or intentional terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by and intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to –

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser" –

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 U.S.C. 2511. Interception and disclosure of wire, oral, or electronic communications prohibited.

(1) Except as otherwise specifically provided in this chapter any person who–

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with–

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents,

landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted–

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter–

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if–

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication–

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted–

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(c)[Redesignated (b)]

(5)(a)(i) If the communication is–

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection–

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

18 U.S.C. 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited.

(1) Except as otherwise specifically provided in this chapter, any person who intentionally–

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of–

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for–

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

18 U.S.C. 2513. Confiscation of wire, oral, or electronic communication interception devices.

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

18 U.S.C. 2515. Prohibition of use as evidence of intercepted wire or oral communications.

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

18 U.S.C. 2516. Authorization for interception of wire, oral, or electronic communications.

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of–

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 (relating to biological weapons) chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of

the United States), section 1116 (relating to protection of foreign officials), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 956 (conspiracy to harm persons or property overseas), section a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents, section 1028A (relating to aggravated identity theft)) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or

(q) any criminal violation of section 229 (relating to chemical weapons): or sections 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism);

(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, , 3); or

(s) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

18 U.S.C. 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications.

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence

while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security act of 1947 (50 U.S.C. 401a), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power of an agent of as foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

18 U.S.C. 2518. Procedure for interception of wire, oral, or electronic communications.

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of

competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that–

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify--

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that–

(a) an emergency situation exists that involves–

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of–

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if–

(a) in the case of an application with respect to the interception of an oral communication--

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication–

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

18 U.S.C. 2519. Reports concerning intercepted wire, oral, or electronic communications.

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts–

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts–

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

18 U.S.C. 2520. Recovery of civil damages authorized.

(a) In general. –Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity other than the United States which engaged in that violation such relief as may be appropriate.

(b) Relief. –In an action under this section, appropriate relief includes–

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages. – (1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of–

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense. –A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation. –A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative Discipline. – If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper Disclosure Is Violation. – Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2510(a).

18 U.S.C. 2521. Injunction against illegal interception.

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

18 U.S.C. 2522. Enforcement of the Communications Assistance for Law Enforcement Act.

(a) Enforcement by court issuing surveillance order. –If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the

carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) Enforcement upon application by Attorney General. –The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) Civil penalty. –
(1) In general. – A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.
(2) Considerations.– In determining whether to impose a civil penalty and in determining its amount, the court shall take into account–
(A) the nature, circumstances, and extent of the violation;
(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and

(c) such other matters as justice may require.

(d) Definitions.– As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

18 U.S.C. 2701. Unlawful access to stored communications.

(a) Offense.–Except as provided in subsection (c) of this section whoever–
(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
(2) intentionally exceeds an authorization to access that facility;
and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment. –The punishment for an offense under subsection (a) of this section is–
(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the constitution and laws of the United States or any state –
(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and
(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and
(2) (A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions. –Subsection (a) of this section does not apply with respect to conduct authorized–
(1) by the person or entity providing a wire or electronic communications service;
(2) by a user of that service with respect to a communication of or intended for that user; or
(3) in section 2703, 2704 or 2518 of this title.

18 U.S.C. 2702. Voluntary disclosure of customer communications or records.

(a) Prohibitions. –Except as provided in subsection (b) or (c) –

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service–

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications. – A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency–

(A) if the contents–

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. P.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

[(C) Repealed. P.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records. –A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) –

(1)as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or

(6) to any person other than a governmental entity.

(d) Reporting of emergency disclosures. –On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing–

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where-–

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

18 U.S.C. 2703. Required disclosure of customer communications or records.

(a) Contents of wire or electronic communications in electronic storage. –A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in a wire or electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b)(1) Contents of electronic communications in a remote computing service. –(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection–

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity–

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service–

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service. –(1)(A) A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).

(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment (including any credit car or bank account number), of a subscriber to or customer of such service, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order. –A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter. –No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence. – (1) In general. – A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention. – Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of Officer not Required. – Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

18 U.S.C. 2704. Backup preservation.

(a) Backup preservation. –(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup

copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of–

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider–

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer challenges. –(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement--

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

18 U.S.C. 2705. Delayed notice.

(a) Delay of notification. –(1) A governmental entity acting under section 2703(b) of this title may–

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is--

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access. –A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in–

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. 2706. Cost reimbursement.

(a) Payment. –Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount. –The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception. –The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

18 U.S.C. 2707. Civil action.

(a) Cause of action. –Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity other than the United States which engaged in that violation such relief as may be appropriate.

(b) Relief. –In a civil action under this section, appropriate relief includes--
(1) such preliminary and other equitable or declaratory relief as may be appropriate;
(2) damages under subsection (c); and
(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages. – The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Administrative Discipline. – If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) Defense. –A good faith reliance on–
(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;
is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation. – A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper Disclosure Is Violation. – Any willful disclosure of a "record", as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official duties of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

18 U.S.C. 2708. Exclusivity of remedies.
The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

18 U.S.C. 2709. Counterintelligence access to telephone toll and transactional records.
(a) Duty to provide–A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification–The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may–
(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of certain disclosure–(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counter terrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.
(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).

(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).

(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).

(d) Dissemination by bureau–The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed–On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(f) Libraries–A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title.

18 U.S.C. 2711. Definitions for chapter.

As used in this chapter–

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.

(4) the term "governmental entity" means a department or agency of the United States or State or political subdivision thereof.

18 U.S.C. 2712. Civil Action against the United States.

(a) In General.– Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes a violation of this chapter or of chapter 119 of this title or of the above special provisions of title 50, the Court may assess as damages–

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures. – (1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried in the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) Administrative Discipline. – If a court or appropriate department or agency determines that the United States or any of the departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) Exclusive Remedy. – Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of Proceedings. – (1) Upon the motion of the united States, the curt shall stay any action commenced under this section f the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms "related criminal case" and "related investigation" means an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether any investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that nay one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

18 U.S.C. 3121. General prohibition on pen register and tape and trace device use; exception.

(a) In general–Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception–The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service–

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

(c) Limitation–A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in identifying the origination or destination of wire or electronic communications.

(d) Penalty–Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

18 U.S.C. 3122. Application for an order for a pen register or a trap and trace device.

(a) Application.(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of application–An application under subsection (a) of this section shall include--

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

18 U.S.C. 3123. Issuance of an order for a pen register or a trap and trace device.

(a) In general. (1) Upon an application made under section 3122(a)(1) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device if the court finds, based on facts contained in the application, that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. Such order shall, upon service of such order, apply to any entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.

(2) Upon an application made under section 3122(a)(2) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds, based on facts contained in the application, that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)(A) Where the law enforcement agency implementing an ex part order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public the agency shall ensure that a record will be maintained which will identify –

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of the such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) Contents of order–An order issued under this section–

(1) shall specify–

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) Time period and extensions–

(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of existence of pen register or a trap and trace device–An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that--

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

18 U.S.C. 3124. Assistance in installation and use of a pen register or a trap and trace device.

(a) Pen registers–Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) Trap and trace device–Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if

such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation–A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(d) No cause of action against a provider disclosing information under this chapter–No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title.

(e) Defense–A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(f) Communications assistance enforcement orders–Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

18 U.S.C. 3125. Emergency pen register and trap and trace device installation.

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(1) an emergency situation exists that involves–

(A) immediate danger of death or serious bodily injury to any person; ~~or~~

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;

that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

18 U.S.C. 3126. Reports concerning pen registers and trap and trace devices.

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning–

(1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
(2) the offense specified in the order or application, or extension of an order;
(3) the number of investigations involved;
(4) the number and nature of the facilities affected; and
(5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

18 U.S.C. 3127. Definitions for chapter.

As used in this chapter–
(1) the terms "wire communication", "electronic communication", "electronic communication service" and "contents" have the meanings set forth for such terms in section 2510 of this title;
(2) the term "court of competent jurisdiction" means–
(A) any district court of the United States (including a magistrate of such a court) or a United States Court of Appeals having jurisdiction over the offense being investigated; or
(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;
(3) the term "pen register" means a device or process which records or decodes or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;
(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;
(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and
(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

Author Contact Information

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968